Oklahoma Testing – Electronic Access Control (EAC) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. What is the main function of the control panel in an EAC system?

A. To issue access credentials

B. To manage data from readers and control locking mechanisms

C. To perform biometric measurements

D. To store system backups

2. What is the primary purpose of visitors' logs in EAC systems?

A. To document the maintenance of security devices

B. To track the number of staff present at all times

C. To maintain a record of who entered and exited a facility and under what conditions for security analysis

D. To monitor the effectiveness of security personnel

3. A REX button must be located within how many feet of a secured door?

A. 2 feet

B. 5 feet

C. 10 feet

D. 15 feet

4. When leaning a ladder against a wall, how far from the wall should the foot of the ladder be located?

A. 1/3 the working length of the ladder

B. 1/4 the working length of the ladder

C. 1/2 the working length of the ladder

D. 1/5 the working length of the ladder

5. Which network technology is predominantly used for mobile communication?

A. GSM

B. Ethernet

C. Wi-Fi

D. Bluetooth

6. According to NFPA 70, direct buried cables must be arranged to prevent?

- **A. Interference from nearby structures**
- **B. Damage when the ground settles**
- **C. Short-circuiting**
- **D. Water accumulation**

7. What is the definition of "credentialing" in the context of electronic access control?

- **A. The process of creating security policies**
- **B. The assignment and management of access credentials**
- **C. The development of access hardware**
- **D. The monitoring of access events**

8. When measuring direct current with a multimeter, what action should be taken first?

- **A. Increase the resistance**
- **B. Disconnect power to the circuit**
- **C. Check for continuity**
- **D. Set to AC measurement**

9. What is an "access control list (ACL)"?

- **A. A list indicating hardware requirements**
- **B. A list that defines the permissions assigned to users or groups for accessing specific resources**
- **C. A directory of all users in the organization**
- **D. A document detailing installation protocols**

10. In relation to EAC systems, what does "cybersecurity" primarily focus on?

- **A. Protecting physical infrastructure**
- **B. Protecting the electronic components of the access control system from unauthorized digital access**
- **C. Enhancing physical security measures**
- **D. Improving user accessibility**

Answers

1. B
2. C
3. B
4. B
5. A
6. B
7. B
8. B
9. B
10. B

Explanations

1. What is the main function of the control panel in an EAC system?

A. To issue access credentials

B. To manage data from readers and control locking mechanisms

C. To perform biometric measurements

D. To store system backups

The main function of the control panel in an Electronic Access Control (EAC) system is to manage data from readers and control locking mechanisms. This centralized component is responsible for processing input from card readers, keypads, or biometric devices that authorize access based on pre-defined permissions. It interprets the data received from these devices to determine whether access should be granted or denied and then sends commands to locking mechanisms to physically secure or unlock entry points. The control panel also plays a critical role in the overall coordination of system components, acting as the hub that ensures the system operates smoothly. Its ability to process real-time data allows for efficient management and monitoring of security protocols, contributing to the safety and security objectives of the facility it serves. This function is essential for maintaining effective access control and responding dynamically to various scenarios, such as alarms or unauthorized access attempts. In contrast, issuing access credentials is typically handled by a separate credentialing system; biometric measurements are performed by dedicated devices designed for that purpose; and while backup databases are important, they do not fall under the core responsibilities of the control panel within an EAC system.

2. What is the primary purpose of visitors' logs in EAC systems?

A. To document the maintenance of security devices

B. To track the number of staff present at all times

C. To maintain a record of who entered and exited a facility and under what conditions for security analysis

D. To monitor the effectiveness of security personnel

In Electronic Access Control (EAC) systems, the primary purpose of visitors' logs is to maintain a record of who entered and exited a facility and under what conditions for security analysis. This functionality is crucial for several reasons. It allows organizations to monitor and account for individuals who are on the premises, enhancing security by providing a clear audit trail. In cases of security breaches or incidents, these logs can offer valuable insights into who may have been present and at what times, facilitating investigations. Furthermore, comprehensive visitor records help organizations assess traffic patterns, identify potential security vulnerabilities, and improve overall safety protocols. Logging visitor access is essential for maintaining accountability and understanding who has authorized entry into specific areas, which is vital for any security framework. This capability distinguishes visits by authorized personnel from unauthorized access attempts, further cementing its role in bolstering an organization's security posture.

3. A REX button must be located within how many feet of a secured door?

A. 2 feet

B. 5 feet

C. 10 feet

D. 15 feet

The correct distance for a REX (Request to Exit) button to be located from a secured door is 5 feet. This specification is set to ensure that individuals can easily access the button when they need to exit the secured area quickly and safely. Placing the button within this distance enhances usability and helps to prevent accidents, as it allows for the button to be within comfortable reach while also maintaining security measures at the door. This requirement operates under the premise of facilitating safe egress for individuals and ensuring the button is not too far away, which could delay exit in an emergency situation. The distance is calibrated to balance safety, security, and accessibility effectively, making 5 feet the ideal standard in most electronic access control scenarios.

4. When leaning a ladder against a wall, how far from the wall should the foot of the ladder be located?

A. 1/3 the working length of the ladder

B. 1/4 the working length of the ladder

C. 1/2 the working length of the ladder

D. 1/5 the working length of the ladder

The correct answer is that the foot of the ladder should be positioned approximately 1/4 the working length of the ladder away from the wall. This 1/4 to 1 ratio is derived from safe ladder placement practices to ensure stability and prevent tipping. When the ladder is anchored correctly, the angle formed with the ground creates a balance that supports both the weight of the person using it and any equipment they may be carrying. Positioning the foot of the ladder at a distance equal to 1/4 the length of the ladder from the wall ensures that the ladder maintains a proper angle, typically around 75 degrees with the ground. This angle is crucial for minimizing the risk of slipping and provides the necessary support for safe climbing. The standard rule emphasizes safety, particularly in preventing accidents that could result from improper ladder placement. In other configurations, such as 1/3, 1/2, or 1/5 of the working length, the ladder may become unstable. A distance of 1/3 could be slightly steep and risk excessive load at the base, while 1/2 would cause the ladder to lean at too shallow an angle, increasing the chance of slipping. Distances less than 1/4, while not

5. Which network technology is predominantly used for mobile communication?

A. GSM

B. Ethernet

C. Wi-Fi

D. Bluetooth

GSM, or Global System for Mobile Communications, is the predominant network technology used for mobile communication. It is widely recognized for its role in mobile phone networks and supports various services, including voice calls and data transmission. GSM technology allows mobile devices to connect to cellular networks, facilitating reliable communication over large distances. In contrast, the other technologies listed serve different purposes. Ethernet is primarily used for wired local area networks (LANs), making it suitable for connecting devices within a local setting but not for mobile communications. Wi-Fi is designed for wireless local area networks, providing internet access over short distances, but it does not support the broader mobile communication that GSM does. Bluetooth is intended for short-range communication between devices, typically for data transfer or connecting peripherals, rather than for extensive mobile communication networks. Thus, while these technologies have their applications, GSM remains the standard for mobile communication on a global scale.

6. According to NFPA 70, direct buried cables must be arranged to prevent?

A. Interference from nearby structures

B. Damage when the ground settles

C. Short-circuiting

D. Water accumulation

The correct answer focuses on preventing damage when the ground settles. This aspect is critical because when cables are directly buried underground, they are subject to various environmental factors and changes in soil conditions, including settling or shifting. If cables are not properly installed or arranged, ground movement can lead to physical stress on the cables, potentially causing insulation damage or even breaking the conductors. To ensure the integrity and safety of the electrical cables, they should be buried at appropriate depths and in conduits when necessary, helping to absorb or mitigate the effects of ground settlement. This preservation of the cable's condition is paramount to maintain functionality and safety, as damaged cables can lead to faults, outages, or hazardous situations. In contrast, while interference, short-circuiting, and water accumulation are relevant issues, they do not directly relate to the primary concern of damage resulting from ground settling. Proper installation tailored to the local environment and soil conditions is essential for protecting against these issues, but the specific concern of preventing damage due to settling underscores the importance of appropriate cable installation methods.

7. What is the definition of "credentialing" in the context of electronic access control?

A. The process of creating security policies

B. The assignment and management of access credentials

C. The development of access hardware

D. The monitoring of access events

In the context of electronic access control, "credentialing" refers to the assignment and management of access credentials. This process involves defining who has permission to access certain areas or information and under what conditions. Access credentials can be physical, such as key cards or biometric data, or digital, like usernames and passwords. Credentialing is essential because it ensures that only authorized individuals can gain entry to secure areas or sensitive information, helping to maintain security integrity within an organization. It entails not only issuing credentials but also keeping track of them, defining user roles, and updating permissions as needed, ultimately forming the backbone of an organization's access control strategy. The other options touch on related aspects of security management but do not encapsulate the concept of credentialing effectively. Creating security policies focuses on the guidelines for behavior and system use, developing access hardware pertains to the physical devices utilized for security measures, and monitoring access events involves observing and recording who accesses what and when, which are all important but distinct from the actual assignment and management of access credentials themselves.

8. When measuring direct current with a multimeter, what action should be taken first?

A. Increase the resistance

B. Disconnect power to the circuit

C. Check for continuity

D. Set to AC measurement

When measuring direct current with a multimeter, it is essential to first disconnect power to the circuit. This action is important for several reasons. First, disconnecting power ensures safety by preventing any electric shock or injury while connecting the multimeter leads to the circuit. It also protects the multimeter itself from damage, especially if the incorrect measurement function is selected. Furthermore, by having the power off before connecting the multimeter, one can accurately set it up without influencing the circuit's operation or producing erroneous measurements. This is particularly crucial in sensitive electronic circuits, where applying voltage or current inadvertently can lead to component failure or incorrect readings. Other options may pertain to significant aspects of measurement but do not represent the critical first step necessary for safely and correctly measuring direct current.

9. What is an "access control list (ACL)"?

A. A list indicating hardware requirements

B. A list that defines the permissions assigned to users or groups for accessing specific resources

C. A directory of all users in the organization

D. A document detailing installation protocols

An access control list (ACL) is fundamentally a list that specifies which users or groups have permission to access particular resources within a system, as well as the types of access they are allowed (such as read, write, or execute permissions). This security mechanism is essential in restricting and managing user access to sensitive information or resources, thus helping to protect data integrity and confidentiality. By using ACLs, administrators can effectively control who can perform specific actions on various resources, which is crucial for maintaining a secure computing environment. For example, in a file system, an ACL will define which users are allowed to view or modify a file and what level of access each user has, thereby preventing unauthorized use or data breaches. This targeted approach to permissions supports organizational policies around data access and user roles. While the other options may pertain to different aspects of information technology or organizational management, they do not accurately describe the function or purpose of an ACL. For instance, indicating hardware requirements, listing all users, or detailing installation protocols do not address the primary function of defining user access rights to resources.

10. In relation to EAC systems, what does "cybersecurity" primarily focus on?

A. Protecting physical infrastructure

B. Protecting the electronic components of the access control system from unauthorized digital access

C. Enhancing physical security measures

D. Improving user accessibility

The primary focus of cybersecurity in relation to Electronic Access Control (EAC) systems is to safeguard the electronic components of those systems from unauthorized digital access. As EAC systems manage the access to physical spaces and resources, they often rely heavily on digital technology—including software, networks, and databases—to function effectively. This digital aspect makes them susceptible to various cybersecurity threats, such as hacking, malware, or data breaches, which could compromise the integrity and effectiveness of the access control measures. By implementing robust cybersecurity practices, organizations can ensure that only authorized personnel can interact with the system, thus maintaining control over access to sensitive areas or information. This focus on protecting the electronic components is essential for retaining the effectiveness of the EAC systems, ensuring they operate reliably and securely while also safeguarding against potential cyber threats that could undermine their operation and security functions. In this context, other choices may touch on important aspects of security, but they do not specifically address the core concern of cybersecurity in EAC systems, which is digital protection.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://oktestingeac.examzify.com

We wish you the very best on your exam journey. You've got this!