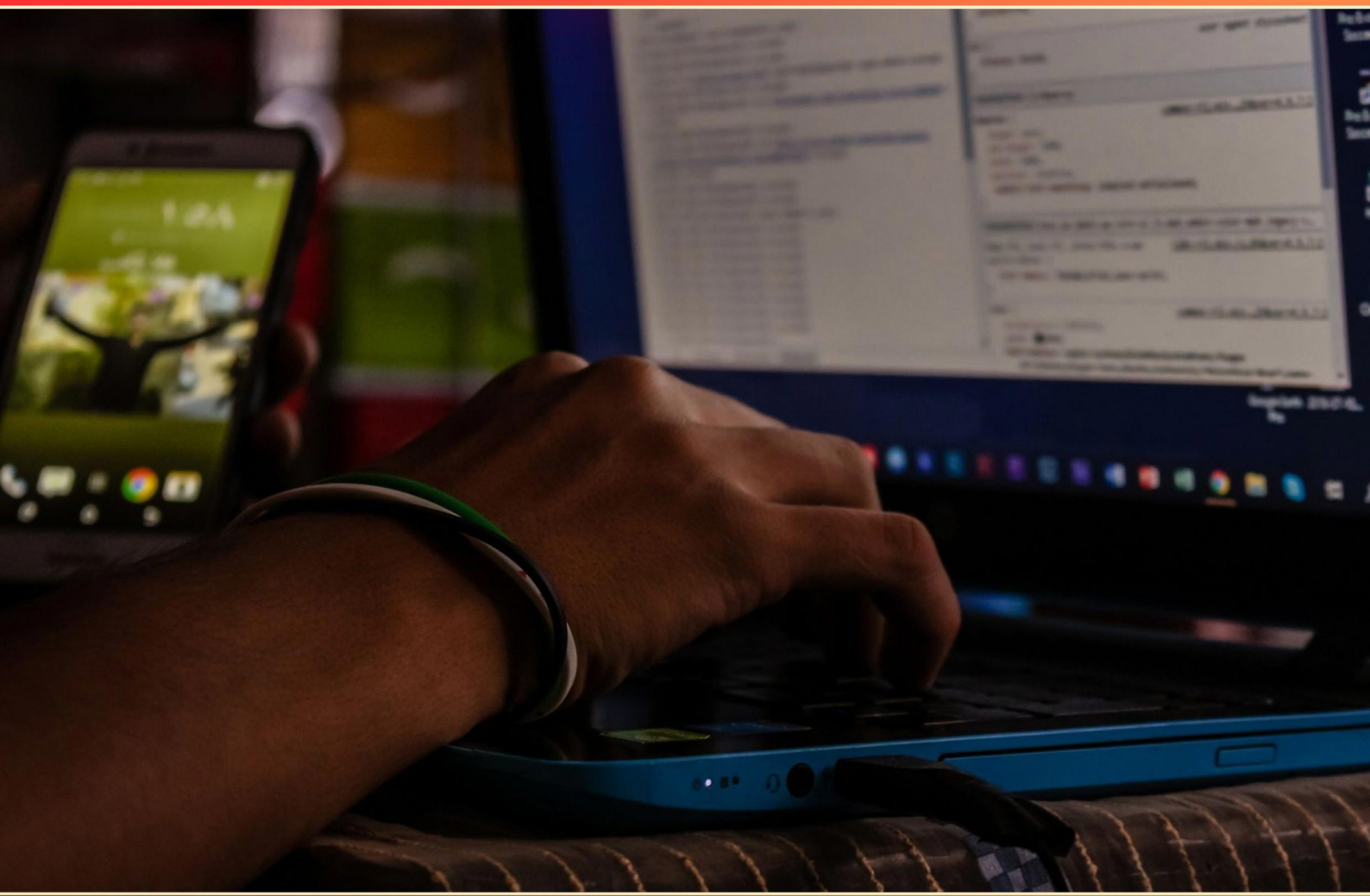
PERFORM USER ACCOUNT MANAGEMENT PHASE 1 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://performuseracctmgmt.examzify.com

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. How would you enforce device compliance before granting access?

A. Device health checks, endpoint management, device inventory, patch status, MDM/EMM.

B. Allow access from any device without checks.

C. Only require password strength.

D. Check device location only.

2. Which practice is consistent with minimizing risk in identity management?

A. Define roles in a central identity provider and propagate them to connected apps via SCIM or provisioning connectors.

B. Use multiple central identity providers with inconsistent roles.

C. Storing credentials in plain text in spreadsheets.

D. Disable RBAC across apps.

3. Why is device-based conditional access important?

A. It ensures all devices have the same OS version.

B. It reduces risk by allowing access only from compliant, managed devices.

C. It guarantees MFA is not needed on any device.

D. It eliminates the need for passwords entirely.

4. Which statement about multifactor authentication (MFA) is true?

A. Adds a second factor to verify identity, mitigating password-only compromises.

B. Replaces the need for any passwords.

C. Requires biometrics for all users in all cases.

D. Makes password complexity irrelevant.

5. PKI stands for?

A. Public Key Infrastructure

B. Private Key Institute

C. Public Infrastructure Key

D. Private Internet Key

6. How do device trust and location influence login access controls?

A. Device posture and geographic location can gate access; enforce device compliance checks, geo/IP restrictions, and context-aware authentication.

B. Rely solely on a user name and password with no device checks.

C. Allow access from any device without policy restrictions.

D. Always require biometric authentication, ignoring device posture.

7. Which of the following is NOT listed as a reason to decommission a user account?

A. Permanent Change of Station (PCS)

B. Expiration Term of Service (ETS)

C. Retirement

D. Transfer

8. Which best describes Cyber Awareness Training focus?

A. Influencing user behavior to mitigate threats and vulnerabilities

B. Understanding vendor risk management

C. Building software development life cycle

D. Configuring routers and switches

9. ATCTS imports training and certification completion data from which DoD systems?

A. Army E-Learning, Virtual Training Website, Fort Eisenhower School House, DoD Virtual Training Environment (VTE), and DoD Workforce Certification Web Application System (DWCA)

B. Local training records only

C. External commercial course catalogs

D. None of the above

10. Which item would best appear in IAM compliance reporting?

A. System uptime

B. Privilege changes

C. Entitlements, remediation status, and access reviews outcomes

D. Weather disruptions

Answers

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

Explanations

1. How would you enforce device compliance before granting access?

A. Device health checks, endpoint management, device inventory, patch status, MDM/EMM.

B. Allow access from any device without checks.

C. Only require password strength.

D. Check device location only.

Enforcing device compliance before granting access hinges on evaluating the device's posture through a set of managed checks. By performing device health checks, you verify that the device is operating normally and free from known issues. Endpoint management and device inventory confirm the device is enrolled, known, and under IT control, so it can be enforced with policies. Patch status ensures the device has current security updates, reducing vulnerability to exploits. MDM/EMM provides the framework to apply and enforce security configurations, such as encryption, passcodes, app controls, and allowed OS versions, and can block access or remediate if noncompliant. When all these criteria are met, access is granted only to devices that meet the security requirements, reflecting a zero-trust approach where trust is based on verified device posture. Relying on any single factor like allowing any device, only requiring a password, or checking location alone does not verify the necessary security state and would leave gaps that attackers could exploit.

2. Which practice is consistent with minimizing risk in identity management?

A. Define roles in a central identity provider and propagate them to connected apps via SCIM or provisioning connectors.

B. Use multiple central identity providers with inconsistent roles.

C. Storing credentials in plain text in spreadsheets.

D. Disable RBAC across apps.

Centralizing identity management and automating provisioning across apps reduces risk by ensuring that access is controlled from one authoritative source and applied consistently everywhere. When roles and permissions are defined in a central identity provider and pushed to connected applications through standards like SCIM or provisioning connectors, changes such as hiring, role changes, or terminations are reflected everywhere in a timely, uniform way. This supports least privilege, reduces the chance of stale or conflicting permissions, and makes auditing and revocation much more reliable. Storing credentials in plain text in spreadsheets is a serious security flaw, exposing sensitive data to leaks or misuse. Using multiple central identity providers with inconsistent roles creates governance gaps and drift in access control. Disabling RBAC removes a foundational mechanism for controlling who can do what across systems, increasing risk dramatically.

3. Why is device-based conditional access important?

A. It ensures all devices have the same OS version.

B. It reduces risk by allowing access only from compliant, managed devices.

C. It guarantees MFA is not needed on any device.

D. It eliminates the need for passwords entirely.

Device-based conditional access gates access to resources based on the security status of the endpoint. When a device is enrolled in management and passes posture checks—such as being encrypted, having a current OS, a valid passcode, and not being jailbroken or rooted—it's considered compliant and allowed to access corporate apps and data. If it isn't compliant, access can be blocked or restricted or require remediation first. This approach reduces risk by ensuring sensitive resources aren't exposed to insecure or unmanaged devices, tying access to both who you are and the trustworthiness of the device you're using. It also aligns with a Zero Trust mindset, where access decisions consider device health alongside user identity. Other options don't fit as well because device-based conditional access doesn't mandate that all devices share the same OS version, and it doesn't remove the need for MFA or passwords. MFA and credentials may still be required; device compliance enhances risk-based access rather than replacing authentication.

4. Which statement about multifactor authentication (MFA) is true?

A. Adds a second factor to verify identity, mitigating password-only compromises.

B. Replaces the need for any passwords.

C. Requires biometrics for all users in all cases.

D. Makes password complexity irrelevant.

Using multiple verification factors strengthens login security by not relying on a single credential. Multifactor authentication combines at least two different types of factors: something you know (a password), something you have (a code from a phone or a hardware token), or something you are (biometrics). The statement that MFA adds a second factor to verify identity, helping protect against password-only compromises, captures this idea: even if a password is stolen, the attacker still needs the additional factor to gain access. MFA does not replace passwords entirely; in most setups the password remains the first factor and a second factor is added. It also doesn't require biometrics for everyone in every case—many implementations use a code from a smartphone or a hardware token instead. And it doesn't make password complexity irrelevant—strong passwords are still important, but MFA adds an extra barrier that greatly reduces risk from password theft.

5. PKI stands for?

A. Public Key Infrastructure

B. Private Key Institute

C. Public Infrastructure Key

D. Private Internet Key

PKI stands for Public Key Infrastructure, a framework that uses public-key cryptography to issue, manage, and revoke digital certificates that bind public keys to identities. This system enables trusted communications by letting others verify who you are, encrypt data for you, and ensure message integrity. At its core, a certificate ties a public key to a real-world identity, and it's issued by a trusted Certification Authority. Supporting pieces like a Registration Authority helps verify identities, and mechanisms such as Certificate Revocation Lists or OCSP handle revocation when a certificate should no longer be trusted. The other phrases aren't standard terms for this concept, so they don't describe the established framework for managing keys and trust. Public Key Infrastructure.

6. How do device trust and location influence login access controls?

A. Device posture and geographic location can gate access; enforce device compliance checks, geo/IP restrictions, and context-aware authentication.

B. Rely solely on a user name and password with no device checks.

C. Allow access from any device without policy restrictions.

D. Always require biometric authentication, ignoring device posture.

Contextual access control uses signals from the device and the login location to decide whether to allow, challenge, or block access. When the device is deemed trusted and compliant—for example, it has current patches, encryption, and proper security posture—and the login comes from an expected geographic area or IP, the system can grant access with normal authentication or apply lighter risk checks. If posture or location signals raise risk, the policy can require additional verification or deny access, reflecting a context-aware approach that adapts to the situation. This approach is better because it adds meaningful security beyond just a username and password, tying access to the actual security state of the device and where the user is coming from. Relying solely on credentials ignores device health and location, making accounts more vulnerable. Allowing access from any device with no policy restrictions removes crucial controls that protect against compromised devices and unusual login from new places. Even though biometrics can be part of a strong authentication flow, ignoring device posture means missing opportunities to adjust risk based on the device itself.

7. Which of the following is NOT listed as a reason to decommission a user account?

A. Permanent Change of Station (PCS)

B. Expiration Term of Service (ETS)

C. Retirement

D. Transfer

In account lifecycle management, decommissioning means removing a user's access because they no longer need it due to leaving or ending their service. The reasons that are listed as triggers for decommissioning include scenarios where the individual's status changes to no longer support continued access: Permanent Change of Station (PCS) and Expiration Term of Service (ETS) reflect a change in assignment or end of service, and Retirement clearly ends active duty. The reason described as a transfer, however, does not end the employment or require removing the person's access; it's a change to a different unit or role within the organization. In that case, you typically update or reallocate the account's scope and permissions rather than decommissioning the account entirely, since the person still needs access in their new position.

8. Which best describes Cyber Awareness Training focus?

A. Influencing user behavior to mitigate threats and vulnerabilities

B. Understanding vendor risk management

C. Building software development life cycle

D. Configuring routers and switches

Cyber Awareness Training centers on shaping how people behave to reduce security risks. It teaches employees to recognize phishing, avoid social engineering, use strong passwords and MFA, and report suspicious activity, turning knowledge into everyday actions that lessen vulnerabilities. This emphasis on the human factor is what makes it the best fit. In contrast, vendor risk management deals with third-party risks, the software development lifecycle focuses on secure software creation, and configuring routers and switches is about network device setup. So the focus on influencing user behavior is the most accurate description.

9. ATCTS imports training and certification completion data from which DoD systems?

A. Army E-Learning, Virtual Training Website, Fort Eisenhower School House, DoD Virtual Training Environment (VTE), and DoD Workforce Certification Web Application System (DWCA)

B. Local training records only

C. External commercial course catalogs

D. None of the above

ATCTS is built to centralize training and certification status by pulling completion records from multiple DoD training systems. When a service member completes a course in Army E-Learning, the Virtual Training Website, Fort Eisenhower School House, the DoD Virtual Training Environment, or the DoD Workforce Certification Web Application System, those completion details are imported into ATCTS so the overall training profile stays current in one trusted place. This cross-system data flow is what makes ATCTS effective for accurate status tracking, reporting, and audits. Local training records alone wouldn't capture all the training activity across DoD, and external commercial catalogs aren't DoD systems feeding into ATCTS. None of the above isn't correct because these DoD sources exist and feed into ATCTS.

10. Which item would best appear in IAM compliance reporting?

A. System uptime

B. Privilege changes

C. Entitlements, remediation status, and access reviews outcomes

D. Weather disruptions

In IAM compliance reporting, you want visibility into the governance of access: who has what entitlements, whether any identified access issues have been remediated, and the outcomes of formal access reviews. This combination shows both the current access state and how governance processes are enforcing compliance. Entitlements describe the permissions granted to users, remediation status shows progress on fixing identified risks (for example, removing unnecessary privileges), and access reviews outcomes provide the results of periodic audits, including approvals, denials, and follow-up actions. System uptime relates to service availability rather than access governance, so it isn't a core part of IAM compliance reporting. Weather disruptions are irrelevant. While privilege changes track changes to permissions, they don't by themselves demonstrate the outcome of governance activities like remediation and review results, which are what compliance reporting emphasizes.

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://performuseracctmgmt.examzify.com

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