TRUSTED AGENT (TA) PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://trustedagent.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. **If you witness a token security violation, which action should be taken first?**

   A. Report the violation to the NETCOM RA Office

   B. Report the violation to the local ISSO

   C. Take no action

   D. Escalate to commanding officer for immediate review

2. **Which statement best explains AAA in a TA context?**

   A. Authentication verifies identity; Authorization grants access rights; Accounting records activity for auditing.

   B. Authentication encrypts data; Authorization logs keystrokes; Accounting hides audit logs.

   C. Authentication skips user verification; Authorization overrides policies; Accounting replaces attestations.

   D. Authentication manages keys; Authorization handles network routing; Accounting handles user training.

3. **Which statement best describes the principle of least privilege in access control?**

   A. Maximize user productivity by default.

   B. Log all user activity for auditing.

   C. Grant users only the minimum level of access necessary to perform their job functions.

   D. Require multifactor authentication for all access.

4. **Which statement accurately describes encryption at rest and encryption in transit?**

   A. In transit protects stored data.

   B. At rest protects stored data; in transit protects data moving across networks; examples: disk encryption for stored files, TLS for web traffic.

   C. At rest protects data moving across networks.

   D. Both protections are the same.

5. **Which RMF activity occurs in Prepare?**

   A. Set up the environment and define boundaries.

   B. Define impact levels.

   C. Select security controls.

   D. Deploy controls.

6. What is chain of custody in digital evidence?

A. Documentation of who handled evidence, when, and how

B. Ownership of the evidence by law

C. How to store evidence physically

D. Chain of custody is irrelevant to TA

7. Which statement describes the function of accounting in access control?

A. To enforce password complexity.

B. To assign user roles.

C. To determine system configurations.

D. To record actions for auditing and traceability.

8. Which of the following items are included in a TA's transaction log?

A. Issued Tokens

B. Recovered or tokens that are turned in

C. Lost Tokens

D. All of the above

9. Which statement is true about token revocation and reissuance?

A. You must revoke active certificates before reissuing a token

B. You can reissue without revoking certificates

C. Revocation is optional

D. Reissuance occurs automatically

10. What does HIPAA require for safeguarding electronic protected health information (ePHI), and how would a TA implement it?

A. Administrative, physical, and technical safeguards; access controls, encryption, audit trails; the TA ensures systems handling ePHI meet HIPAA requirements and maintain attestations.

B. HIPAA requires only encryption; the TA sells encryption services.

C. HIPAA concerns only financial transactions; the TA focuses on billing security.

D. HIPAA is a general data privacy law with no specific safeguards; the TA ignores compliance.

Answers

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

Explanations

1. If you witness a token security violation, which action should be taken first?

A. Report the violation to the NETCOM RA Office

B. Report the violation to the local ISSO

C. Take no action

D. Escalate to commanding officer for immediate review

The first thing to do is report the incident to the designated security authority so it can be logged and handled properly from the outset. Reporting to the NETCOM RA Office ensures the event goes into the official record and is triaged by the team responsible for initial assessment and escalation. They coordinate with the right security stakeholders, including the local ISSO, to guide follow-on actions. Taking no action is not acceptable, and bypassing the official reporting path by escalating directly to a commanding officer can delay proper containment and coordination. Reporting to the NETCOM RA Office sets the right process in motion from the start.

2. Which statement best explains AAA in a TA context?

A. Authentication verifies identity; Authorization grants access rights; Accounting records activity for auditing.

B. Authentication encrypts data; Authorization logs keystrokes; Accounting hides audit logs.

C. Authentication skips user verification; Authorization overrides policies; Accounting replaces attestations.

D. Authentication manages keys; Authorization handles network routing; Accounting handles user training.

AAA in a TA context focuses on three functions: Authentication confirms who is trying to access resources, Authorization determines what that user is allowed to do, and Accounting records the actions taken for auditing and accountability. The statement that Authentication verifies identity, Authorization grants access rights, and Accounting records activity for auditing directly maps to these three roles, making it the best explanation of AAA. Other options mix in concepts that aren't part of AAA, such as encryption or keystroke logging, or suggest actions like skipping verification or hiding audit logs, which don't describe the AAA framework.

3. Which statement best describes the principle of least privilege in access control?

A. Maximize user productivity by default.

B. Log all user activity for auditing.

C. Grant users only the minimum level of access necessary to perform their job functions.

D. Require multifactor authentication for all access.

The principle of least privilege means giving each user the minimum access rights they need to perform their job tasks. This limits what a user can do or access, so even if their account is compromised or an error is made, the potential damage is kept small. It also makes it easier to enforce separation of duties and to audit who has access to what, since permissions are restricted to what's strictly necessary for their role. For example, a software developer might need access to the code repository and development tools, but not access to payroll data or HR records. An everyday user might only need to view certain files, not modify sensitive configurations. Granting only these minimal rights aligns with secure, responsible access management. The other options describe related concepts but don't capture the core idea. Maximizing productivity by default would grant too many privileges. Logging all user activity relates to auditing, not to the level of access granted. Requiring multifactor authentication strengthens identity verification, but it doesn't specify restricting privileges once identity is established.

4. Which statement accurately describes encryption at rest and encryption in transit?

A. In transit protects stored data.

B. At rest protects stored data; in transit protects data moving across networks; examples: disk encryption for stored files, TLS for web traffic.

C. At rest protects data moving across networks.

D. Both protections are the same.

Encryption at rest and encryption in transit address different moments of data life. Encryption at rest protects data when it's stored on devices, databases, or backups—so even if someone gains access to the storage medium, the data remains unreadable. Disk encryption and database-level encryption are common examples that keep stored files safe. Encryption in transit protects data as it moves across networks. This guards against eavesdropping or tampering while data travels between systems, clients, and servers. TLS for web traffic is a standard example, ensuring confidential and integral transfer of information. The statement captures this distinction by saying at rest protects stored data and in transit protects data moving across networks, with disk encryption for stored files and TLS for web traffic as concrete examples. The other options mix up where each protection applies or claim they're the same, which isn't accurate.

5. Which RMF activity occurs in Prepare?

A. Set up the environment and define boundaries.

B. Define impact levels.

C. Select security controls.

D. Deploy controls.

In RMF, the Prepare phase is about getting everything ready and setting the scope for the process. That means setting up the environment, identifying the system, its boundaries, interfaces, and the roles and responsibilities of everyone involved, along with how risk will be managed. Defining boundaries and establishing the environment lays the groundwork for all subsequent steps, ensuring that categorization, control selection, and deployment are done against a clear, correctly scoped system. Defining impact levels is done during the categorization step, where you determine the potential impact on the organization's operations, assets, and individuals. Selecting security controls comes next, in the control selection step. Deploying controls occurs later when implementing and applying those controls.

6. What is chain of custody in digital evidence?

A. Documentation of who handled evidence, when, and how

B. Ownership of the evidence by law

C. How to store evidence physically

D. Chain of custody is irrelevant to TA

Chain of custody for digital evidence is the documented history of how that evidence has been handled from collection onward. It records who handled it, when they did so, and how the evidence was preserved, transferred, or accessed, often including copies, hash verifications, and storage details. This trail helps prove the evidence hasn't been altered and supports its reliability and admissibility by showing a transparent sequence of custody. Ownership by law is about legal rights to the item and isn't the same as the procedural log of who touched the evidence. Storing it properly is important, but chain of custody covers every action and transfer, not just storage. It's a fundamental practice in digital investigations, including for trusted agent work.

7. Which statement describes the function of accounting in access control?

A. To enforce password complexity.

B. To assign user roles.

C. To determine system configurations.

D. To record actions for auditing and traceability.

Accounting in access control is about recording what happens when users interact with the system. It creates an audit trail—the who, what, when, and where of actions—so you can trace activities back to individuals and times. This logging supports accountability, incident response, and regulatory compliance by making it possible to review events after the fact. The other aspects address different functions: enforcing password complexity relates to authentication policy, assigning user roles is about authorization, and determining system configurations is a matter of system administration. Recording actions for auditing and traceability best describes accounting in access control.

8. Which of the following items are included in a TA's transaction log?

A. Issued Tokens

B. Recovered or tokens that are turned in

C. Lost Tokens

D. All of the above

Complete visibility of token movements is what the TA transaction log aims to provide. A robust log should capture issued tokens to show what has entered circulation, recovered or tokens that are turned in to return tokens to the system or remove them from active use, and lost tokens to flag discrepancies and prevent fraud or double counting. Each of these events affects the overall token inventory and accountability in different ways, so including all of them gives the most accurate, auditable record. If any one category were omitted, gaps could emerge where issues, recoveries, or losses aren't tracked, undermining reconciliation and security. Therefore, the most comprehensive choice is to include all of the above.

9. Which statement is true about token revocation and reissuance?

A. You must revoke active certificates before reissuing a token

B. You can reissue without revoking certificates

C. Revocation is optional

D. Reissuance occurs automatically

When managing tokens, revoking the current credential before issuing a replacement is the standard approach to prevent abuse. Revoking marks the active token as invalid so that services validating the token will reject it, and the new token becomes the only valid credential. If you reissue without revoking, the old token remains usable for a while, creating a window where both tokens could be accepted and could be misused if the old one were compromised. In secure systems, revocation isn't optional—you rely on revocation lists or status checks to invalidate tokens that should no longer be trusted. Reissuance isn't typically automatic; it's a controlled process that occurs in response to a request or policy, coordinated with revocation to ensure the old token can no longer be used.

10. What does HIPAA require for safeguarding electronic protected health information (ePHI), and how would a TA implement it?

A. Administrative, physical, and technical safeguards; access controls, encryption, audit trails; the TA ensures systems handling ePHI meet HIPAA requirements and maintain attestations.

B. HIPAA requires only encryption; the TA sells encryption services.

C. HIPAA concerns only financial transactions; the TA focuses on billing security.

D. HIPAA is a general data privacy law with no specific safeguards; the TA ignores compliance.

HIPAA's Security Rule requires a comprehensive set of safeguards across administrative, physical, and technical controls to protect electronic protected health information. A TA would implement this by first conducting a risk assessment to identify vulnerabilities and determine applicable safeguards. Administrative safeguards include clear access policies, least-privilege access, security training for staff, incident response, and contingency planning. Physical safeguards involve secure facility controls, device protection, media handling, and proper disposal of equipment with ePHI. Technical safeguards cover measures like unique user IDs and authentication, access controls to ensure only authorized personnel can view ePHI, encryption of data in transit and at rest where appropriate, and robust audit controls and logging to monitor and detect access or alterations. Documentation and attestations of compliance help demonstrate ongoing adherence, and ensuring business associates meet these requirements is part of the implementation. Other options fall short because encryption alone isn't sufficient, HIPAA addresses more than financial transactions, and it provides specific safeguard requirements rather than treating privacy as a general, non-prescriptive rule.

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://trustedagent.examzify.com

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