Trusted Agent (TA) 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 are the OWASP Top 10 and why are they relevant to a TA?

A. They are the most critical web app security risks (for example, injection, broken authentication, sensitive data exposure); the TA uses them to guide testing and control enforcement.

B. They are a list of hardware vulnerabilities; the TA uses them to fix devices.

C. They are a set of licensing requirements; the TA uses them to manage software licenses.

D. They are a coding style guide; the TA uses them to standardize naming.

2. 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.

3. The Trusted Agent must protect from theft, loss or unauthorized access to which of the following?

A. Computer equipment, software and supplies

B. Cryptographic modules

C. Tokens

D. All of the above

4. What is the TA role in attestation data and logs during threat detection?

A. Ensure provenance of attestation data and logs

B. Generate attestations without validation

C. Delete logs after use

D. Ignore attestation data

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 the role of Trusted Agents (TAs)?

- **A. To conduct security audits**
- **B. To provide the interface between the Army RA and Subscribers/PKI Sponsors**
- **C. To manage network hardware**
- **D. To develop PKI policies**

7. Under what circumstances must a TA be terminated?

- **A. If they request a transfer to another department**
- **B. If they are late to work three times**
- **C. If they are arrested**
- **D. If they fail to meet the criteria in DA Pamphlet 25-2-13**

8. What should a Subscriber do if their PIN or token is compromised?

- **A. Wait 24 hours before reporting**
- **B. Report the compromise immediately**
- **C. Change their password and continue using the token**
- **D. Attempt to fix the token themselves**

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. Which statement describes the process when a token's certificate expires?

A. Revocation request submitted to RA office

B. Token continues to work

C. PIN can be reset

D. Certificate is renewed automatically

Answers

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

Explanations

1. What are the OWASP Top 10 and why are they relevant to a TA?

A. They are the most critical web app security risks (for example, injection, broken authentication, sensitive data exposure); the TA uses them to guide testing and control enforcement.

B. They are a list of hardware vulnerabilities; the TA uses them to fix devices.

C. They are a set of licensing requirements; the TA uses them to manage software licenses.

D. They are a coding style guide; the TA uses them to standardize naming.

The OWASP Top 10 is a widely recognized catalog of the most critical web application security risks. It highlights risk areas that attackers commonly exploit, such as injection flaws, broken authentication, and sensitive data exposure. For a Trusted Agent, this list provides a practical framework to guide testing and control enforcement—focusing efforts on the vulnerabilities most likely to cause harm and ensuring test scenarios reflect real-world attack patterns. It helps with risk-based planning: you prioritize test cases around these risks, assess whether defenses like input validation, secure authentication, access controls, and encryption are in place, and offer remediation guidance. It also supports threat modeling and clear communication with stakeholders by providing a shared vocabulary. Note that it does not cover hardware vulnerabilities, licensing, or coding style; those areas lie outside the Top 10. The Top 10 is periodically updated to reflect evolving threats, so staying current keeps testing relevant.

2. 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.

3. The Trusted Agent must protect from theft, loss or unauthorized access to which of the following?

A. Computer equipment, software and supplies

B. Cryptographic modules

C. Tokens

D. All of the above

Assets that support secure operation must be protected from theft, loss, or unauthorized access. This includes tokens that store authentication credentials, cryptographic modules that safeguard keys and cryptographic operations, and computer equipment, software, and supplies that can contain sensitive data or enable system breaches. If any one of these asset categories is compromised, an attacker could gain credentials, decrypt data, or take control of systems. Because every item on the list can be a vulnerability, the trusted agent must protect all of them—All of the above.

4. What is the TA role in attestation data and logs during threat detection?

A. Ensure provenance of attestation data and logs

B. Generate attestations without validation

C. Delete logs after use

D. Ignore attestation data

The main idea here is that threat detection relies on trustworthy evidence, so preserving the origin and integrity of attestation data and logs is essential. Attestation data provide a verifiable snapshot of a system's state, and logs capture events over time; their usefulness hinges on being able to trust where they came from and that they haven't been altered. The trusted agent's role is to ensure provenance—confirming the source of the data, its authenticity, and that a tamper-evident chain of custody is maintained—so security systems can rely on the information when detecting threats or investigating incidents. If attestations are produced without validation, or if logs are deleted or ignored, the evidence becomes unreliable and threat detection and response weaken. Therefore, ensuring provenance of attestation data and logs is the best approach.

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 the role of Trusted Agents (TAs)?

A. To conduct security audits

B. To provide the interface between the Army RA and Subscribers/PKI Sponsors

C. To manage network hardware

D. To develop PKI policies

Trusted Agents serve as the bridge between the Army's Registration Authority and the people or organizations enrolling in the PKI. They handle enrollment requests from subscribers, verify identity and eligibility according to PKI rules, and then pass the verified information to the Registration Authority for certificate issuance. They also work with PKI sponsors to understand and meet sponsor requirements, translating those needs into practical enrollment actions and provisioning. This mediating role ensures smooth, compliant certificate enrollment and lifecycle management by connecting end users with the RA. These tasks aren't about conducting security audits, managing network hardware, or drafting PKI policies, which are handled by separate teams or roles.

7. Under what circumstances must a TA be terminated?

A. If they request a transfer to another department

B. If they are late to work three times

C. If they are arrested

D. If they fail to meet the criteria in DA Pamphlet 25-2-13

This question tests understanding of when a Trusted Agent must be terminated according to policy. A TA must be terminated when they fail to meet the criteria defined in DA Pamphlet 25-2-13. Those criteria set the essential qualifications, conduct standards, and safeguards necessary to maintain trust and security in the role. If someone does not meet those standards, removal from the position is required to protect the integrity of the program. Other scenarios like transferring to another department, consistent lateness, or an arrest may lead to disciplinary actions or investigations, but they do not by themselves mandate termination under this policy. Only failing to meet the specified criteria in the DA pamphlet requires termination.

8. What should a Subscriber do if their PIN or token is compromised?

A. Wait 24 hours before reporting

B. Report the compromise immediately

C. Change their password and continue using the token

D. Attempt to fix the token themselves

When credentials like a PIN or security token are compromised, reporting it immediately is essential to contain the breach. Prompt notification allows security to revoke or invalidate the compromised token, reset the PIN if needed, and monitor for unusual activity across accounts and sessions. Acting quickly reduces the window of opportunity for an attacker to misuse the credentials and access sensitive data or systems. Simply changing a password won't automatically neutralize the threat if the token itself remains in the attacker's hands or could be reused for authentication. Trying to fix the token yourself can lead to misconfigurations or leave the system in a vulnerable state; official remediation steps are needed. So, reporting right away to the security team or IT help desk is the best course to minimize damage and restore secure access.

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. Which statement describes the process when a token's certificate expires?

A. Revocation request submitted to RA office

B. Token continues to work

C. PIN can be reset

D. Certificate is renewed automatically

When a certificate reaches its expiration date, it stops being valid for use. Expiration simply marks that the certificate can no longer be trusted after that point, so the token must obtain a new certificate to continue securely authenticating or signing. Revocation, on the other hand, is a mechanism used to invalidate a certificate before its scheduled expiry—typically because the private key was compromised or the certificate should no longer be trusted for some other reason. It's not the process triggered by expiration. So, the normal remedy for an expired certificate is to renew or reissue the certificate so the token can again be trusted. Some systems may support automatic renewal if configured, but that depends on policy. The idea behind expiration is renewal, not revocation.

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!