Threat Awareness and Reporting Program (TARP) Practice Exam (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 a typical next step after completing a TARP investigation?**
   - **A. Publicly disclose the findings.**
   - **B. Archive the case with no actions.**
   - **C. Only report to law enforcement with no further actions.**
   - **D. Determine appropriate actions based on facts and risk assessment.**

2. **Who pled guilty to attempted spear phishing cyber-attack on Department of Energy Computers?**
   - **A. Mustafa Awwad**
   - **B. John Doe**
   - **C. Charles Eccleston**
   - **D. Jane Smith**

3. **Under DODD 5240.06, Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors; which of the following is not reportable?**
   - **A. Contact with Known or Suspected Foreign Intelligence**
   - **B. Removing of classified markings**
   - **C. Unexplained or undue affluence**
   - **D. None of these**

4. **Which of the following are collection methods used by adversaries?**
   - **A. Cyber Attacks**
   - **B. Solicitation and Marketing of Services**
   - **C. Unsolicited Requests for Information**
   - **D. All of the above**

5. **What is a key benefit of timely reporting under TARP?**
   - **A. It supports timely assessment and response to protect people and property.**
   - **B. It guarantees job advancement for the reporter.**
   - **C. It eliminates all risk.**
   - **D. It reduces the need for a formal investigation.**

6. Which statement about anomalies is accurate?

A. Anomalies are suspicious patterns that warrant investigation.

B. They are normal routines with no risk.

C. All anomalies indicate espionage with certainty.

D. They are always identified by risk assessment teams.

7. Which of the following are potential espionage indicators?

A. Unusual work hours

B. Concealing foreign travel

C. Unexplained affluence

D. All of the above

8. Being invited to lecture or attend a conference in a foreign country is one potential indicator of foreign entity targeting.

A. True

B. False

C. Not an indicator on its own

D. Only if paired with other indicators

9. A Security Anomaly is best described as?

A. A routine operational procedure.

B. Foreign power or activity or knowledge inconsistent with the expected norm.

C. An internal memo.

D. A public press release.

10. As government employees, our greatest vulnerabilities are those things we take for granted.

A. False

B. Sometimes True

C. True

D. Not Applicable

Answers

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

Explanations

1. What is a typical next step after completing a TARP investigation?

A. Publicly disclose the findings.

B. Archive the case with no actions.

C. Only report to law enforcement with no further actions.

D. Determine appropriate actions based on facts and risk assessment.

The next step after a TARP investigation is to determine appropriate actions based on the facts uncovered and the level of risk they present. This means evaluating what happened and then deciding how to respond in a way that reduces harm, prevents recurrence, and strengthens controls—such as remedying gaps, updating policies, enhancing training, adjusting processes, or escalating to authorities if warranted. Public disclosure or simply archiving without action can create further risk or misalignment with governance, and reporting only to law enforcement might miss internal remediation opportunities. Acting on a facts-and-risk basis ensures a proportional, justified response that protects stakeholders and improves the program.

2. Who pled guilty to attempted spear phishing cyber-attack on Department of Energy Computers?

A. Mustafa Awwad

B. John Doe

C. Charles Eccleston

D. Jane Smith

Understanding this item hinges on recognizing that targeted cyber intrusions into government networks can lead to criminal charges, even if the attacker doesn't succeed in breaching the system. When someone pleads guilty to an attempted spear phishing attack on Department of Energy computers, it shows that prosecutors treat the act as a serious crime and hold individuals accountable for trying to compromise critical infrastructure. The person named—Charles Eccleston—is the individual who admitted guilt in this case, illustrating how the plea process works and the kind of offense involved: attempting to deceive legitimate users to gain access to protected systems. Spear phishing involves crafting personalized messages to specific targets to steal credentials or install malware, a common initial step in broader cyber campaigns against important networks. This case highlights the real-world legal consequences that can follow such actions, especially when directed at federal infrastructure. The other names are not connected to this particular plea, which is why the named individual is the correct reference in this scenario.

3. Under DODD 5240.06, Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors; which of the following is not reportable?

A. Contact with Known or Suspected Foreign Intelligence

B. Removing of classified markings

C. Unexplained or undue affluence

D. None of these

The question tests which behaviors must be reported under the DoD policy for foreign intelligence contacts and indicators. Under DODD 5240.06, each of the items described is considered a reportable warning sign. A contact with known or suspected foreign intelligence is itself a red flag that security personnel need to review. Removing classified markings is a serious breach of how sensitive information is handled and signals potential exposure or intent to misuse classified material, so it must be reported. Unexplained or undue affluence can point to coercion, bribery, or foreign influence, which also warrants reporting to assess risk and intervene. Since all three examples are reportable, there isn't anything on the list that would be not reportable, making the correct interpretation that none of these are excluded from reporting.

4. Which of the following are collection methods used by adversaries?

A. Cyber Attacks

B. Solicitation and Marketing of Services

C. Unsolicited Requests for Information

D. All of the above

Adversaries gather information through multiple channels to learn about targets, assets, and weaknesses. Each method fits a different angle of collection: cyber attacks directly breach systems to access data and exfiltrate it; soliciting and marketing of services can be a pretext to lure personnel, gather sensitive details, or gain legitimate access under the guise of a vendor or consultant; unsolicited requests for information exploit social engineering to elicit confidential data or credentials from individuals or teams. Because information can be obtained through technical breaches, social interaction, or credible-seeming business contexts, all of these methods are used in information collection. To defend, strengthen cyber defenses, implement rigorous vendor risk management and verification for third-party inquiries, and train people to recognize and appropriately handle unsolicited information requests and social-engineering attempts.

5. What is a key benefit of timely reporting under TARP?

A. It supports timely assessment and response to protect people and property.

B. It guarantees job advancement for the reporter.

C. It eliminates all risk.

D. It reduces the need for a formal investigation.

Timely reporting under TARP matters because it enables responders to quickly assess the situation and respond to protect people and property. When information arrives promptly, security teams and emergency services can gauge threat severity, decide what protective actions are needed, and mobilize resources fast—such as evacuations, shelter-in-place, medical aid, or targeted security measures—before harm escalates. This direct link to rapid protection is the core benefit. Promotions or career advancement aren't tied to safety reporting, and reporting doesn't eliminate all risk; investigations may still be needed to verify facts and guide next steps, but a timely report starts the right actions sooner.

6. Which statement about anomalies is accurate?

A. Anomalies are suspicious patterns that warrant investigation.

B. They are normal routines with no risk.

C. All anomalies indicate espionage with certainty.

D. They are always identified by risk assessment teams.

Anomalies are patterns that appear unusual when compared with what's expected or with established baselines. The point is to flag deviations that warrant closer scrutiny and possible investigation, not to declare danger immediately. They signal potential risk and invite further analysis, correlation with other indicators, and additional evidence gathering. Normal routines with no risk aren't anomalies, because anomalies are deviations from the normal pattern. Saying all anomalies indicate espionage with certainty is incorrect because many anomalies are benign, due to error or legitimate exceptions. And while risk assessment teams play a key role in evaluating risk, anomalies aren't always identified only by them; they can be detected by automated monitoring, frontline observations, or other processes that flag unusual activity for review.

7. Which of the following are potential espionage indicators?

A. Unusual work hours

B. Concealing foreign travel

C. Unexplained affluence

D. All of the above

The key idea is that espionage indicators come from patterns of suspicious behavior, travel, and finances that could signal someone is connected to foreign intelligence or handling sensitive information improperly. Unusual work hours can indicate someone trying to observe or access information outside normal oversight, especially if the timing aligns with access windows or sensitive tasks. Concealing foreign travel raises concern about contacts with foreign entities or activities that aren't disclosed, which can be a sign of compromised loyalties or information exchange. Unexplained affluence—sudden wealth or expensive lifestyle changes without a clear, legitimate source—can point to illicit funding or favors that might be linked to espionage activities. When these indicators appear together, they form a stronger red flag than any single item alone, which is why all of the listed indicators are considered potential espionage indicators. They are warnings to be reported and investigated, not proof on their own.

8. Being invited to lecture or attend a conference in a foreign country is one potential indicator of foreign entity targeting.

A. True

B. False

C. Not an indicator on its own

D. Only if paired with other indicators

Being invited to lecture or attend a conference in a foreign country signals cross-border engagement with foreign audiences and institutions, which is a common way foreign entities try to identify, cultivate, or influence individuals of interest. This outreach can create legitimate opportunities, but in threat awareness, it also serves as a potential indicator that a foreign actor is attempting to build connections, map networks, or gain access to information or influence. The invitation moves the target into an international spotlight or network where foreign actors can gauge credibility, establish rapport, and open lines of contact for future collaboration or pressure. Because it demonstrates exposure to foreign actors and settings, it should be treated as a potential indicator of foreign targeting and investigated further, especially if seen alongside other indicators such as unusual funding, recurring travel to foreign events, or access requests to sensitive information.

9. A Security Anomaly is best described as?

A. A routine operational procedure.

B. Foreign power or activity or knowledge inconsistent with the expected norm.

C. An internal memo.

D. A public press release.

A security anomaly is something that stands out as unusual or unexpected compared to what normally happens. The description that fits best is foreign power or activity or knowledge inconsistent with the expected norm because it pinpoints the kind of irregular signal security teams watch for—actions, influences, or information that don't fit the usual pattern and could indicate a threat. This helps highlight potential risks like espionage, unauthorized access, or compromised assets. The other options describe normal, everyday items: a routine operational procedure is expected behavior, an internal memo is standard internal communication, and a public press release is external and not inherently suspicious. None of these imply the irregular, norm-violating signal that a security anomaly is meant to flag.

10. As government employees, our greatest vulnerabilities are those things we take for granted.

A. False

B. Sometimes True

C. True

D. Not Applicable

Taking security for granted creates a blind spot that threats can exploit. When government employees perform routine tasks, work with familiar systems, or handle common information, we can slip into autopilot and skip safeguards we would normally follow. That complacency opens doors to social engineering, mishandling of sensitive data, or weaker access controls simply because nothing feels urgent or out of the ordinary. The strength of security rests on disciplined, everyday behavior; if those practices lapse because we assume "it's fine," the most significant vulnerabilities emerge. So, this statement is true: our greatest vulnerabilities are often the things we take for granted because they reflect how we actually operate, not how we should operate under ideal conditions.

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://threatawarenessrepprog.examzify.com

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