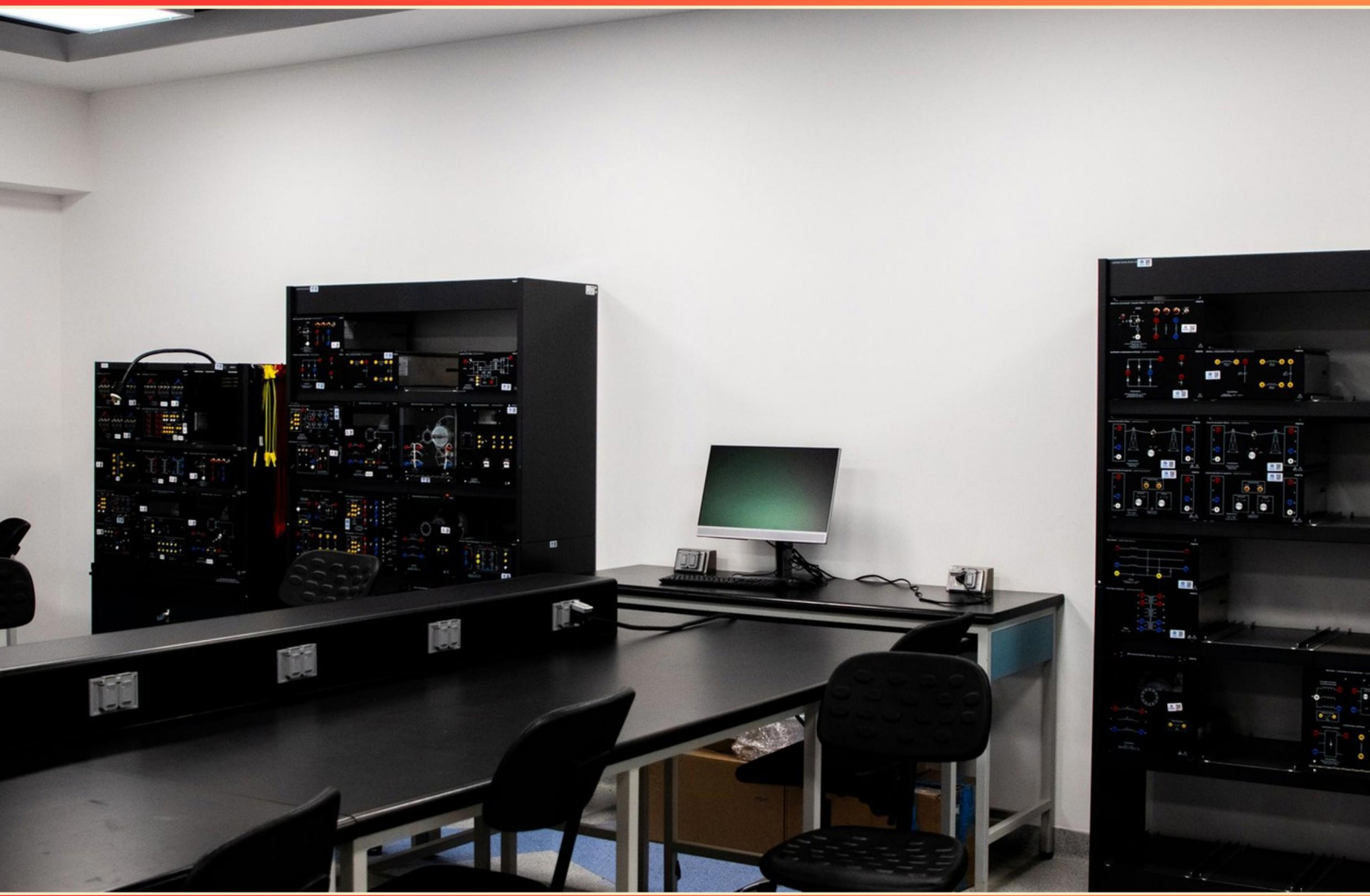
# DEPARTMENT OF DEFENSE (DOD) INFORMATION SECURITY AND INSIDER THREAT PRACTICE TEST (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://dod-informationsecurityandinsiderthreat.examzify.com

**Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.**

**ALL RIGHTS RESERVED.**

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

# Table of Contents


Copyright ..... 1

Table of Contents ..... 2

Introduction ..... 3

How to Use This Guide ..... 4

Questions ..... 5

Answers ..... 8

Explanations ..... 10

Next Steps ..... 16


SAMPLE

# 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.

SAMPLE

# 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!

SAMPLE

# Questions

SAMPLE

1. **Which behavior is considered a reportable indicator of potential security issues?**

   A. Regularly attending work

   B. Significant change in work habits

   C. Consistently punctual arrivals

   D. Engaging in team-building activities

2. **Who should you report to if contacted by the media about sensitive information?**

   A. Your supervisor

   B. Your colleagues

   C. Your security office

   D. Legal department

3. **Which of the following should contractors report to the insider threat program?**

   A. Personal grievances

   B. Efforts to obtain unauthorized access to classified information

   C. Annual performance reviews

   D. Training compliance issues

4. **When should classified information be considered for declassification?**

   A. When it is damaged

   B. When it is no longer deemed necessary for national security

   C. When there is a risk of loss

   D. When new legislation is passed

5. **What should be done to classify information as Top Secret?**

   A. It must be highly sensitive and unauthorized disclosure could cause exceptional damage

   B. It must be reviewed monthly

   C. It can only be classified based on external requests

   D. It requires general security awareness training

SAMPLE

**6. Which of the following is considered a potential insider threat vulnerability?**

A. Substance abuse

B. Disgruntlement

C. Gambling addiction

D. All of the above

**7. What are the key activities of an insider threat detection program?**

A. Monitoring user activity and managing software licenses

B. Monitoring user activity and analyzing behavioral patterns

C. Conducting physical security audits and granting access

D. Reviewing employee reports and increasing workforce size

**8. In the context of information security, what should a security officer be most vigilant about?**

A. Employee performance ratings

B. Contractual obligations of personnel

C. Behavioral changes indicating potential threats

D. Compliance with regular audits

**9. What is a key aspect of maintaining cyber hygiene?**

A. Regularly sharing passwords among staff

B. Updating software and systems consistently

C. Limiting technology usage to business hours

D. Using personal devices for work purposes

**10. What does the term 'compilation' refer to in the context of information classification?**

A. Combining classified documents

B. Classifying unclassified information at a higher level

C. Creating summary reports for classified information

D. Reviewing unauthorized disclosures

SAMPLE

# Answers

SAMPLE

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

SAMPLE

# Explanations

SAMPLE

## 1. Which behavior is considered a reportable indicator of potential security issues?

A. Regularly attending work

B. Significant change in work habits

C. Consistently punctual arrivals

D. Engaging in team-building activities

*A significant change in work habits serves as a crucial reportable indicator of potential security issues because it may signify underlying problems that could impact both the individual and the organization. Such changes can include alterations in productivity levels, shifts in workload management, or unexpected absences. These behavioral shifts may indicate stress, dissatisfaction, or engagement in concerning activities, which could pose a risk to information security or enterprise integrity. Being vigilant about changes in work behavior aligns with the broader goal of early detection in insider threat programs, enabling timely intervention before any substantial harm occurs to the organization or its data. Observing and reporting these significant changes help create a more secure environment, allowing for proactive measures to mitigate risks associated with insider threats.*

## 2. Who should you report to if contacted by the media about sensitive information?

A. Your supervisor

B. Your colleagues

C. Your security office

D. Legal department

*Reporting to the security office when contacted by the media about sensitive information is essential for several reasons. The security office is specifically trained to handle incidents involving sensitive data and can provide the necessary guidance on how to navigate media inquiries. They are responsible for ensuring that information is disclosed appropriately and in accordance with policies and regulations designed to protect national security and organizational integrity. Additionally, the security office has protocols in place for managing communications with outside parties, such as the media, and can help prevent unauthorized disclosures that might compromise sensitive information. This step ensures that any information shared is controlled and consistent with official messaging, which is crucial in maintaining the organization's credibility and compliance with legal obligations. While the legal department might also play a role in ensuring that any communications comply with regulations, the immediate responsibility for handling media inquiries lies with the security office. They are equipped to evaluate the potential risks and implications of any information that could be disclosed and will coordinate with other relevant departments when necessary.*

SAMPLE

## 3. Which of the following should contractors report to the insider threat program?

A. Personal grievances

B. Efforts to obtain unauthorized access to classified information

C. Annual performance reviews

D. Training compliance issues

*Contractors should report efforts to obtain unauthorized access to classified information to the insider threat program because this type of behavior poses a significant risk to national security. The insider threat program is designed to identify, mitigate, and respond to potential threats from individuals who have authorized access to sensitive or classified information. When there are attempts—whether successful or not—to gain unauthorized access, it indicates a potential insider threat, which needs to be monitored and addressed to protect against data breaches, espionage, or other malicious activities. This reporting is crucial for maintaining the integrity and security of sensitive information, ensuring that the appropriate measures are taken to investigate and prevent any threats to the organization or national security. The insider threat program relies on vigilance from all employees, including contractors, to keep the information environment secure and to act upon any suspicious actions promptly.*

## 4. When should classified information be considered for declassification?

A. When it is damaged

B. When it is no longer deemed necessary for national security

C. When there is a risk of loss

D. When new legislation is passed

*The consideration for declassification of classified information centers around the continuation of its necessity for national security. When classified information is determined to no longer be essential for protecting national security interests, it becomes appropriate to declassify that information. This can occur due to various factors, including changes in political or military circumstances, advancements in technology, or shifts in public knowledge that render the information less sensitive or relevant. For example, intelligence that was once critical may become outdated or irrelevant as time passes, leading to a reassessment of its classification status. This approach ensures that the classification system remains dynamic and responsive to the current needs of national security while also promoting transparency where possible. Other options do not align with the established criteria for declassification. Damage to the material, the risk of loss, or the passing of legislation does not inherently suggest that the information should be declassified; these factors may lead to different courses of action rather than a reevaluation of its classification status. Thus, the essence of national security requirements directly informs the declassification process.*

SAMPLE

## 5. What should be done to classify information as Top Secret?

A. It must be highly sensitive and unauthorized disclosure could cause exceptional damage

B. It must be reviewed monthly

C. It can only be classified based on external requests

D. It requires general security awareness training

*To classify information as Top Secret, it must indeed be highly sensitive, with the potential for exceptional damage to national security if disclosed without authorization. The criteria for granting Top Secret classification are stringent, ensuring that only the most sensitive information that, if revealed, could severely harm the United States or its allies can be designated as such. The significance of this classification level is underscored by the requirement that information needing this designation would likely cause grave harm to national security interests, such as compromising intelligence operations, capabilities, or the safety and lives of individuals. Consequently, it is vital for those making classification decisions to thoroughly assess the potential impact of unauthorized disclosures. The other options do not align with the established criteria for Top Secret classification. For instance, reviewing information monthly, classifying solely based on external requests, or requiring only general security awareness training do not meet the stringent requirements necessary to designate information as Top Secret. Each of these alternatives lacks the necessary focus on the sensitivity and potential damage that warrant such a high classification.*

## 6. Which of the following is considered a potential insider threat vulnerability?

A. Substance abuse

B. Disgruntlement

C. Gambling addiction

D. All of the above

*The selection of "All of the above" as the correct answer is valid because each of the listed factors—substance abuse, disgruntlement, and gambling addiction—can significantly contribute to insider threat vulnerabilities within an organization. Substance abuse can impair judgment and decision-making, leading individuals to engage in risky behaviors that could compromise sensitive information or systems. For example, an employee under the influence may act out of character, potentially exposing data or resources. Disgruntlement refers to feelings of dissatisfaction or resentment within the workplace. Employees who feel undervalued, mistreated, or overlooked may be more inclined to commit harmful acts, such as leaking sensitive information or sabotaging systems, as a means of expressing their frustration. Gambling addiction can lead to financial distress, prompting individuals to seek illicit means to obtain money, which may include stealing data or selling confidential information to offset their financial losses. The desperation that follows from such an addiction can compromise an employee's loyalty to the organization. Recognizing these factors is critical in assessing and mitigating risks associated with insider threats, as they create conditions that may drive individuals to engage in harmful actions against the organization. Understanding these potential vulnerabilities aids in developing effective prevention and response strategies within the realm of information security.*

SAMPLE

## 7. What are the key activities of an insider threat detection program?

A. Monitoring user activity and managing software licenses

B. Monitoring user activity and analyzing behavioral patterns

C. Conducting physical security audits and granting access

D. Reviewing employee reports and increasing workforce size

*An insider threat detection program primarily focuses on identifying activities and behaviors that could indicate a potential threat from within the organization. Monitoring user activity is a fundamental aspect of this program, as it allows for the observation of actions taken by users that may deviate from typical behavior, helping to highlight any potentially malicious intentions or negligence. In addition to monitoring, analyzing behavioral patterns plays a crucial role in understanding what constitutes normal user behavior versus what could be considered a threat. This involves employing various analytical techniques to establish baselines of normal activity, which can then be used to detect anomalies that may indicate a security risk. By focusing on user activity and behavioral analysis, organizations can implement proactive measures to thwart potential threats before they materialize, ensuring both data security and protection of critical assets. In contrast, other activities mentioned, such as managing software licenses and conducting physical security audits, do not directly contribute to the detection of insider threats but rather pertain to broader operational efficiency and physical security management, respectively. Reviewing employee reports may help identify issues, but it lacks the proactive element of monitoring and analyzing ongoing behaviors that are essential for effective insider threat detection.*

## 8. In the context of information security, what should a security officer be most vigilant about?

A. Employee performance ratings

B. Contractual obligations of personnel

C. Behavioral changes indicating potential threats

D. Compliance with regular audits

*A security officer should be most vigilant about behavioral changes indicating potential threats because such changes can serve as critical indicators of insider threats. Employees exhibiting unusual behavior—such as increased secrecy, sudden disengagement, or unusual requests for data access—can signal potential security risks. Recognizing and addressing these changes proactively can help prevent breaches of sensitive information and protect the organization from insider threats. While employee performance ratings, contractual obligations, and compliance with audits are important aspects of managing a secure environment, they do not directly indicate an employee's likelihood of engaging in harmful behaviors. Focusing on behavioral indicators allows security personnel to intervene before issues escalate, thereby enhancing the overall security posture of the organization. Monitoring behaviors rather than solely relying on procedural compliance ensures that potential threats are identified and mitigated early, preserving the integrity and confidentiality of the organization's information.*

SAMPLE

## 9. What is a key aspect of maintaining cyber hygiene?

A. Regularly sharing passwords among staff

B. Updating software and systems consistently

C. Limiting technology usage to business hours

D. Using personal devices for work purposes

*Updating software and systems consistently is a critical aspect of maintaining cyber hygiene because it helps protect against vulnerabilities that can be exploited by cyber threats. Cyber hygiene refers to the practices and steps that organizations implement to maintain the health of their digital systems and data. Regular updates often include security patches that rectify known vulnerabilities, address bugs, and enhance system performance. By keeping software and systems up to date, organizations can reduce the risk of cyber incidents, thereby ensuring the integrity, confidentiality, and availability of their data. This proactive approach is essential in an environment where cyber threats are constantly evolving and becoming more sophisticated. In contrast, sharing passwords among staff can lead to security breaches, and limiting technology usage to business hours doesn't inherently secure systems outside those hours. Additionally, using personal devices for work can introduce security risks through unregulated access to sensitive information. Thus, consistent software updates form a foundational element of robust cyber hygiene practices.*

## 10. What does the term 'compilation' refer to in the context of information classification?

A. Combining classified documents

B. Classifying unclassified information at a higher level

C. Creating summary reports for classified information

D. Reviewing unauthorized disclosures

*The term "compilation" in the context of information classification specifically refers to the process of taking unclassified information and combining it in such a manner that it raises the overall classification level. When unclassified pieces of information are compiled together, they may reveal critical insights or sensitive details that, while individually unclassified, create a more comprehensive picture that warrants a classified designation when aggregated. This is crucial in safeguarding national security interests, as it highlights how previously innocuous information can, when viewed together, pose risks that necessitate a higher level of protection. While the other options might relate to information handling or reporting, they do not capture the essence of what "compilation" signifies in information classification. The essence lies in how the act of merging different pieces of information affects their classification status, emphasizing the need for vigilance concerning how data is aggregated and analyzed within the security framework.*

SAMPLE

# 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://dod-informationsecurityandinsiderthreat.examzify.com

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

SAMPLE