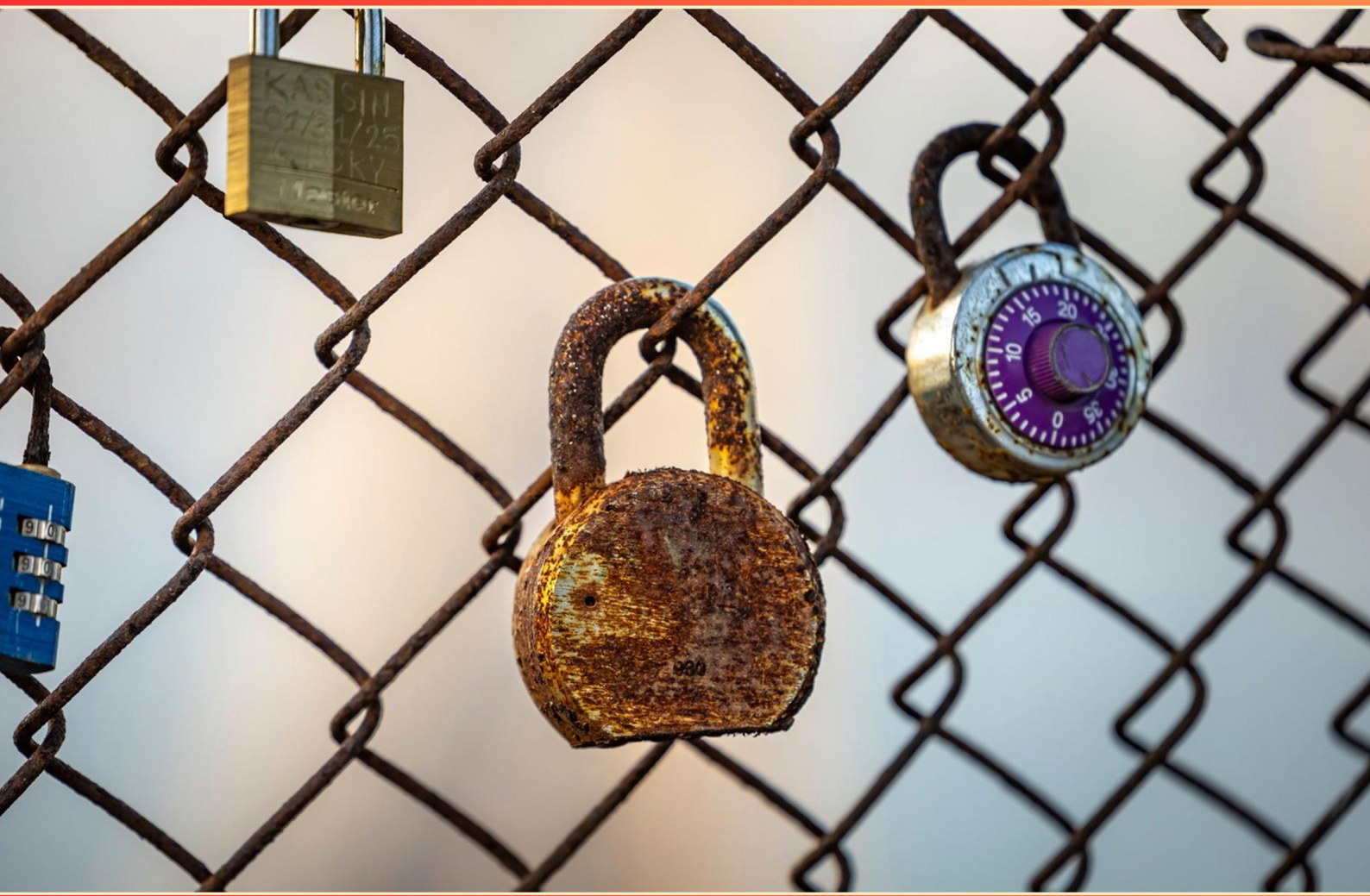
DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dodinstruction520048cui.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. The second line of the designation indicator must identify?

A. The office making the determination.

B. The DoD Component determining the info.

C. All types/categories of CUI contained in the document.

D. The distribution statement or dissemination controls.

2. What are the two main CUI categories used under the policy?

A. Top Secret and Secret.

B. CUI Basic and CUI Specified.

C. Unclassified and Classified.

D. Public and Restricted.

3. Before disclosing CUI to another party, what must you verify?

A. Recipient's department.

B. Recipient authorization and need to know.

C. Recipient's security clearance regardless of need.

D. Only the recipient's name.

4. Under what conditions may CUI be stored on personal devices?

A. It is always allowed on personal devices with a password.

B. It is never allowed on personal devices.

C. Only if policy explicitly allows it and proper safeguards (encryption, access controls, and approvals) are in place.

D. It is allowed if the device is company-owned.

5. What is decontrol of CUI?

A. To add more safeguards.

B. To reclassify as top secret.

C. The process to remove CUI safeguards when information no longer requires protection or restricted dissemination.

D. To transfer to another owner.

SAMPLE

6. What action is required if a CUI container is lost or stolen?

A. Notify a coworker first, then report later.

B. Wait 24 hours before reporting.

C. Immediately report incident to the designated official and initiate protective actions.

D. Document internally and do not report.

7. How should hotlines or reporting channels be used for CUI concerns?

A. Use designated channels to report suspected mishandling or security incidents promptly and securely.

B. Post on social media about concerns.

C. Email any coworker you suspect.

D. Wait until quarterly review.

8. What are the main safeguarding controls in DoD 5200.48?

A. Physical safeguards only.

B. Administrative safeguards only.

C. Technical safeguards only.

D. Physical, administrative, and technical safeguards, plus training and incident response.

9. What is the purpose of the splash screen for systems containing CUI?

A. To log user activity for audits.

B. To alert users of CUI within the program/system and obtain consent.

C. To display system uptime.

D. To provide contact information.

10. What are the destruction requirements for CUI?

A. Destroy CUI materials so they cannot be reconstructed or retrieved, using approved methods.

B. Delete from one device and leave others

C. Archive for archival purposes

D. Delete after five years

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. The second line of the designation indicator must identify?

A. The office making the determination.

B. The DoD Component determining the info.

C. All types/categories of CUI contained in the document.

D. The distribution statement or dissemination controls.

The second line of the designation indicator communicates how the information may be shared. It specifies the distribution statement or dissemination controls that govern who can receive the material and how it can be further disseminated. This line is all about handling and sharing restrictions, not about who created or determined the content. The first line would typically identify the originator or the DoD Component responsible for the document, while the second line locks in the dissemination limits so recipients know whether they may forward, copy, or release the material to others. Listing all types or categories of CUI is not the purpose of the second line; those categories are noted elsewhere.

2. What are the two main CUI categories used under the policy?

A. Top Secret and Secret.

B. CUI Basic and CUI Specified.

C. Unclassified and Classified.

D. Public and Restricted.

The policy uses two main CUI designations: CUI Basic and CUI Specified. CUI Basic is the default category for Controlled Unclassified Information that doesn't have a more restrictive designation, applying standard protection and marking requirements across agencies. CUI Specified is used when information needs additional controls due to statutory, policy, or program-specific restrictions, signaling more stringent handling and access limitations beyond the Basic level. Together, they define how most CUI is treated and when extra safeguards are required. Options referring to Top Secret or Secret relate to classified information, not CUI. The broad terms Unclassified and Classified aren't the formal CUI categories. Public and Restricted aren't official CUI categories either.

3. Before disclosing CUI to another party, what must you verify?

A. Recipient's department.

B. Recipient authorization and need to know.

C. Recipient's security clearance regardless of need.

D. Only the recipient's name.

Before disclosing CUI, you must verify the recipient's security clearance. This clearance acts as the essential gatekeeper for handling sensitive information, ensuring that only individuals who have been vetted to a level appropriate for the data can access it. Even if someone has a stated need to know, without the proper clearance they should not receive CUI, because access must be tied to both authorization and appropriate safeguarding. While confirming authorization and need-to-know is important, the clearance check is the fundamental step that determines whether disclosure can proceed. Relying on department, or simply knowing the recipient's name, does not establish that the information is being shared with someone qualified to handle it.

SAMPLE

4. Under what conditions may CUI be stored on personal devices?

A. It is always allowed on personal devices with a password.

B. It is never allowed on personal devices.

C. Only if policy explicitly allows it and proper safeguards (encryption, access controls, and approvals) are in place.

D. It is allowed if the device is company-owned.

Storing CUI on a personal device is allowed only when there is explicit authorization in policy and the device meets specific safeguards. In practice, this means the organization must authorize personal-device use for CUI and require protections such as encryption of data at rest and in transit, strong access controls (including multi-factor authentication and least-privilege access), formal approvals from the information owner, and ongoing protections like device management, timely patching, and the ability to remotely wipe or terminate access if the device is lost or compromised. These measures ensure CUI remains protected even outside traditional work devices and provide auditable assurances that risk is being managed. The idea that CUI can always be stored on personal devices with only a password isn't enough because passwords alone can be compromised, especially if a device is lost or stolen. The notion that it's never allowed ignores the reality that many organizations permit BYOD under controlled conditions. The suggestion that it's allowed only on company-owned devices misses the scenario being considered and ignores the explicit policy and safeguards required for personal devices.

5. What is decontrol of CUI?

A. To add more safeguards.

B. To reclassify as top secret.

C. The process to remove CUI safeguards when information no longer requires protection or restricted dissemination.

D. To transfer to another owner.

Decontrol of CUI means removing the protective controls that apply to Controlled Unclassified Information when the information no longer requires special protection or restricted dissemination. It's the formal process of lifting CUI safeguards so the information can be treated with standard, less restrictive handling. This is why it's the right answer: decontrol is about ending the special protections, not increasing them, not upgrading the designation to top secret, and not transferring ownership. Adding safeguards would be the opposite of decontrol, reclassifying to top secret would elevate the protection, and transferring ownership is about who handles the information, not how it's protected.

SAMPLE

6. What action is required if a CUI container is lost or stolen?

A. Notify a coworker first, then report later.

B. Wait 24 hours before reporting.

C. Immediately report incident to the designated official and initiate protective actions.

D. Document internally and do not report.

Immediate reporting to the designated official and initiating protective actions is required when a CUI container is lost or stolen. This ensures the incident triggers the approved response process right away, so the organization can quickly determine what data was present, who had access, and what steps are needed to contain and mitigate the risk. Protective actions may include securing the location, revoking or changing access, locating or recovering the media, and notifying the appropriate stakeholders and authorities as required. Delaying reporting or handling the situation informally can leave sensitive information exposed and hamper timely containment and risk assessment. Informing a coworker first delays official escalation, waiting 24 hours increases exposure risk, and simply documenting the incident without reporting fails to activate the necessary containment and notification steps.

7. How should hotlines or reporting channels be used for CUI concerns?

A. Use designated channels to report suspected mishandling or security incidents promptly and securely.

B. Post on social media about concerns.

C. Email any coworker you suspect.

D. Wait until quarterly review.

Using designated hotlines or reporting channels to raise CUI concerns ensures reports are captured, triaged, and escalated quickly and securely. These channels are designed to protect sensitive information while routing the issue to the right security and compliance teams, so remediation can start promptly and an auditable trail is created for accountability. Prompt reporting helps contain potential mishandling and supports timely investigations and corrective action, which is essential for maintaining CUI protection and regulatory compliance. Bypass options like social media or informal emails, which can publicly disclose sensitive data, spread information in uncontrolled ways, and circumvent the official incident response process. Waiting until a quarterly review similarly delays detection and response, increasing risk to the information. When using the designated channel, include relevant details per policy (what happened, when, where, who's involved) and preserve any evidence to aid the investigation.

SAMPLE

8. What are the main safeguarding controls in DoD 5200.48?

A. Physical safeguards only.

B. Administrative safeguards only.

C. Technical safeguards only.

D. Physical, administrative, and technical safeguards, plus training and incident response.

Safeguarding controls rely on a layered, comprehensive approach that spans physical, administrative, and technical measures. Physical safeguards protect the actual environment and equipment—things like controlled access to facilities, locks, and secure rooms. Administrative safeguards cover the governance side—policies, risk management, personnel security, access approvals, and ongoing training to ensure people follow the rules. Technical safeguards are the technology tools that enforce protection—encryption, strong authentication, access controls, monitoring, and auditing of systems and data. DoD 5200.48 emphasizes not only these three domains but also the need for training and an incident response capability. Training ensures individuals know how to handle information securely and recognize risks, while incident response procedures provide a prepared, coordinated way to detect, respond to, and recover from incidents. Because of this integrated, multi-faceted approach, the best answer includes physical, administrative, and technical safeguards plus training and incident response. Options that focus on only one domain miss essential parts of the protection framework and the requirement for proactive training and incident handling.

9. What is the purpose of the splash screen for systems containing CUI?

A. To log user activity for audits.

B. To alert users of CUI within the program/system and obtain consent.

C. To display system uptime.

D. To provide contact information.

Splash screens on systems that contain CUI are there to warn users that they are entering an environment that stores or processes controlled information and to obtain their acknowledgment of and agreement to follow the CUI handling rules and monitoring in place. This notice helps ensure that only authorized individuals access the system and understand their responsibilities, including how the data must be handled and that activity may be monitored. Logging user activity, uptime displays, or contact info are not the primary purpose of this notice: audit trails handle logs, uptime is unrelated to CUI awareness, and contact details alone don't convey the required consent and handling obligations.

SAMPLE

10. What are the destruction requirements for CUI?

A. Destroy CUI materials so they cannot be reconstructed or retrieved, using approved methods.

B. Delete from one device and leave others

C. Archive for archival purposes

D. Delete after five years

Destruction and disposition of CUI are governed by formal procedures that ensure information cannot be reconstructed or retrieved once it is no longer needed. The main idea is that CUI must be disposed of securely when it no longer serves a purpose, using approved methods, unless there is a formal authorization to preserve it for archival purposes. Archiving for archival purposes is the best fit here because, when information has enduring value or is required for historical records, it can be designated for archival retention under approved disposition instructions rather than destroyed. This mirrors the concept that destruction isn't automatic in every case; there are controlled exceptions where preserving the material is authorized and appropriate. Destroying only on one device, deleting after a fixed period, or treating destruction as a unilateral action without a formal disposition plan all fail to capture the authorized pathway for long-term preservation that the policy allows. The option to archive for archival purposes reflects the approved, intentional retention path for CUI when not destroying it.

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://dodinstruction520048cui.examzify.com

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

SAMPLE