CERTIFIED CMMC ASSESSOR (CCA) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cmmcaassessor.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. What is included in a Service Level Agreement (SLA)?

A. Details on service pricing models

B. A list of all employees under the service provider

C. Types and standards of services to be offered

D. A guide for marketing the services provided

2. What is required for an artifact to be considered acceptable evidence in a CMMC assessment?

A. It must be documented by an external auditor

B. It must demonstrate combat readiness

C. It must show implementation of relevant processes

D. It must be signed by organizational leadership

3. Subnetworks in a network architecture are primarily used for what purpose?

A. To allow unrestricted access across the entire network

B. To create distinct functional segments with controlled access

C. To centralize user authentication processes

D. To ensure full connectivity among all devices

4. What function does access control policies serve?

A. They define the physical layout of facilities

B. They govern user interactions with systems and resources

C. They perform system updates automatically

D. They restrict all data access

5. What governs the types of services outlined in a Service Level Agreement?

A. Market competition

B. Internal company policies

C. The expressed needs of the customer

D. The capabilities of technology vendors

SAMPLE

6. What is the purpose of a Non-Disclosure Agreement (NDA) in the CMMC assessment?

A. To outline the assessment timeline

B. To protect sensitive information exchanged during the assessment

C. To define assessment roles and responsibilities

D. To disclose the assessment findings to third parties

7. What is a fundamental practice for maintaining organizational systems?

A. Adopting a reactive maintenance approach

B. Prioritizing aesthetic improvements

C. Establishing a proactive maintenance schedule

D. Focusing solely on electronic systems

8. What is prohibited in terms of information system use according to legal notifications?

A. Authorized use of systems

B. Collaboration with other users

C. Unauthorized use of information systems

D. Access through temporary accounts

9. What is the main purpose of a C3PAO being listed as "authorized" or "accredited" in the CMMC Marketplace?

A. To allow C3PAOs to conduct Level 2 assessments

B. To provide training for organizations

C. To facilitate online workshops

D. To issue CMMC certification badges

10. What tool is used to help establish context for CMMC Assessment activities?

A. A compliance checklist

B. A Data Flow Diagram

C. An employee assessment form

D. An incident response plan

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is included in a Service Level Agreement (SLA)?

A. Details on service pricing models

B. A list of all employees under the service provider

C. Types and standards of services to be offered

D. A guide for marketing the services provided

A Service Level Agreement (SLA) is a formal document that outlines the relationship between a service provider and a customer, specifically detailing the types of services to be delivered and the standards for those services. This includes important elements such as response time for service requests, service availability, performance metrics, and what the customer can expect in terms of quality. By clearly defining the types and standards of services, the SLA helps to manage expectations and provides a framework for measuring the service provider's performance. This clarity is vital for both parties, as it ensures that they are aligned in their understanding of the obligations and commitments involved in the service relationship. In contrast to the correct answer, the inclusion of details on service pricing models, a list of all employees under the service provider, and marketing guides does not fall within the main objectives of an SLA. While pricing may be a consideration in contractual agreements, it is generally addressed separately from the specifics of service delivery standards.

2. What is required for an artifact to be considered acceptable evidence in a CMMC assessment?

A. It must be documented by an external auditor

B. It must demonstrate combat readiness

C. It must show implementation of relevant processes

D. It must be signed by organizational leadership

For an artifact to be considered acceptable evidence in a CMMC assessment, it is essential that it demonstrates the implementation of relevant processes. This ensures that the evidence is grounded in real practices and activities that the organization has carried out in relation to the Cybersecurity Maturity Model Certification requirements. Artifacts that illustrate how security controls are put into practice provide verifiable proof that the organization not only has policies in place but is actively following them. This verification is crucial for assessors as they evaluate an organization's compliance with the specific CMMC model level. In addition, showing implementation helps in establishing a link between documented procedures and actual behavior, which is important for the integrity of the assessment process. This kind of direct evidence allows assessors to evaluate the effectiveness of a company's cybersecurity posture and its ability to protect Controlled Unclassified Information (CUI). The other options do not align with this fundamental requirement. While documentation from an external auditor, combat readiness, or signatures from leadership may hold significance in other contexts, they do not directly provide evidence of active implementation of security processes necessary for CMMC compliance.

SAMPLE

3. Subnetworks in a network architecture are primarily used for what purpose?

A. To allow unrestricted access across the entire network

B. To create distinct functional segments with controlled access

C. To centralize user authentication processes

D. To ensure full connectivity among all devices

Subnetworks, or subnets, are utilized in network architectures primarily to create distinct functional segments with controlled access. This segmentation enhances security and performance by isolating different areas of the network based on their specific roles or functional requirements. For instance, a network might be divided into subnets for different departments within an organization, such as finance, human resources, and IT. Each subnet can have tailored access controls, limiting which users can access certain resources based on their roles. Implementing subnetting allows for improved management of network traffic and the application of specific security measures to each segment. This means that even if a breach occurs in one subnet, the impact can be contained without affecting other parts of the network. Furthermore, it aids in efficient IP address management and can help boost overall network performance by reducing congestion. The other choices do not accurately reflect the primary purpose of subnetting. Unrestricted access across an entire network can lead to security vulnerabilities; centralizing user authentication is not the main focus of subnetting; and while connectivity among devices is important, the creation of distinct segments is essential for security and management rather than ensuring full connectivity.

4. What function does access control policies serve?

A. They define the physical layout of facilities

B. They govern user interactions with systems and resources

C. They perform system updates automatically

D. They restrict all data access

Access control policies serve the critical function of governing user interactions with systems and resources. These policies establish the rules and guidelines that dictate how users can access, interact with, and manage information and system resources. They determine who is allowed to access certain data, what level of access they have (such as read, write, or modify permissions), and ensure that sensitive information is only available to authorized personnel. By implementing access control policies, organizations can protect their data from unauthorized access and potential breaches, thereby maintaining confidentiality, integrity, and availability of their information systems. Such policies are essential for compliance with various standards and regulations, including those delineated in cybersecurity frameworks like the CMMC, which emphasizes the importance of managing access rights effectively. The other choices do not accurately capture the primary purpose of access control policies. Choices that reference physical layout or system updates are unrelated to access control, while the idea of restricting all data access contradicts the necessity of allowing controlled access to users who are authorized. Thus, option B most accurately reflects the role of access control policies in an organization's security framework.

SAMPLE

5. What governs the types of services outlined in a Service Level Agreement?

A. Market competition

B. Internal company policies

C. The expressed needs of the customer

D. The capabilities of technology vendors

The correct answer emphasizes the importance of understanding the expressed needs of the customer within the framework of a Service Level Agreement (SLA). An SLA is fundamentally a contract that specifies the expected service levels, quality, and responsibilities between a service provider and a customer. By focusing on the customer's needs, the SLA becomes a tailored document that reflects the specific requirements and expectations that the customer has for the services being provided. This alignment with customer needs ensures that the services outlined are relevant and useful, ultimately leading to higher satisfaction and better performance outcomes. When the service levels are designed based on the customer's expectations, it also helps in setting clear criteria for measurement and evaluation of the service provided. While market competition, internal company policies, and the capabilities of technology vendors certainly influence the overall environment in which SLAs are crafted, they do not govern the specific services outlined. The core of an SLA should prioritize the customer's requirements to ensure its effectiveness and relevance.

6. What is the purpose of a Non-Disclosure Agreement (NDA) in the CMMC assessment?

A. To outline the assessment timeline

B. To protect sensitive information exchanged during the assessment

C. To define assessment roles and responsibilities

D. To disclose the assessment findings to third parties

The purpose of a Non-Disclosure Agreement (NDA) in the context of a CMMC assessment is primarily focused on protecting sensitive information that is exchanged during the assessment process. In this scenario, the NDA legally binds all parties involved to confidentiality, ensuring that proprietary or sensitive data shared amongst assessors and organizations is safeguarded against unauthorized disclosure. By establishing clear boundaries around the handling of sensitive information, the NDA helps maintain trust between the organization undergoing assessment and the assessors, which is crucial for a thorough and transparent review process. This confidentiality is particularly important in the CMMC framework, as it often deals with Controlled Unclassified Information (CUI) and requires a robust mechanism to prevent data breaches or misuse. While others might relate to aspects of the assessment process, such as timelines or roles, these do not capture the primary function of an NDA, which is centered exclusively on confidentiality and the secure management of sensitive information. Thus, option B is the most accurate representation of the NDA's purpose in this context.

SAMPLE

7. What is a fundamental practice for maintaining organizational systems?

A. Adopting a reactive maintenance approach

B. Prioritizing aesthetic improvements

C. Establishing a proactive maintenance schedule

D. Focusing solely on electronic systems

Establishing a proactive maintenance schedule is a fundamental practice for maintaining organizational systems because it involves planning and performing regular maintenance activities before issues arise. This approach allows organizations to identify and address potential problems early, reducing downtime and ensuring that systems operate efficiently and effectively. By proactively maintaining systems, organizations can enhance their reliability and longevity, leading to overall better performance and reduced costs associated with emergency repairs and system failures. This practice also contributes to achieving compliance with various regulatory requirements, including those related to cybersecurity, by ensuring that systems are consistently updated and monitored, thereby reducing vulnerabilities. A proactive approach fosters a culture of continuous improvement and accountability, which is crucial for organizational resilience and operational excellence.

8. What is prohibited in terms of information system use according to legal notifications?

A. Authorized use of systems

B. Collaboration with other users

C. Unauthorized use of information systems

D. Access through temporary accounts

The prohibition of unauthorized use of information systems is crucial for maintaining the security and integrity of organizational data. Unauthorized use refers to any access or use of information systems by individuals who do not have explicit permission or authority to do so. This can lead to various risks, including data breaches, theft of sensitive information, and potential legal liabilities for the organization. Legal notifications often outline the responsibilities and restrictions imposed on users to protect the organization's information assets. These notifications are designed to ensure that all users are aware of their rights and duties regarding system access. In this context, emphasizing the need to avoid unauthorized use reinforces the idea that only those with appropriate clearance or authorization should interact with the systems. The other options provided generally refer to activities that are acceptable or expected within the guidelines of authorized access and collaboration. Authorized use and collaboration among users are typically permitted as long as they comply with established security protocols. Accessing systems through temporary accounts may be regulated, but it is not inherently prohibited. Thus, the main focus here is on the clear and necessary prohibition of unauthorized access to safeguard information systems.

SAMPLE

9. What is the main purpose of a C3PAO being listed as "authorized" or "accredited" in the CMMC Marketplace?

A. To allow C3PAOs to conduct Level 2 assessments

B. To provide training for organizations

C. To facilitate online workshops

D. To issue CMMC certification badges

The primary purpose of a Cybersecurity Maturity Model Certification (CMMC) Third Party Assessment Organization (C3PAO) being listed as "authorized" or "accredited" in the CMMC Marketplace is to enable them to conduct assessments at various maturity levels, including Level 2. When a C3PAO is recognized as authorized, it signifies that they have met the rigorous standards set forth by the CMMC Accreditation Body. This accreditation ensures that the organization has the necessary expertise, training, and capability to accurately assess compliance with the CMMC standards, thereby providing confidence to the entities relying on these assessments. The accreditation process is designed to ensure that C3PAOs maintain the integrity, reliability, and quality of the assessments they perform. Thus, being listed as authorized allows these organizations to fulfill their critical role in the CMMC ecosystem, where they provide the necessary assessments to certify organizations seeking to work with the Department of Defense and other federal contracts.

10. What tool is used to help establish context for CMMC Assessment activities?

A. A compliance checklist

B. A Data Flow Diagram

C. An employee assessment form

D. An incident response plan

A Data Flow Diagram is essential for establishing context in CMMC Assessment activities because it visually represents how data moves within an organization, highlighting where sensitive information is stored, processed, and transmitted. This becomes crucial for understanding potential vulnerabilities, ensuring compliance with the CMMC framework, and identifying the appropriate security measures needed to protect Controlled Unclassified Information (CUI). By mapping out data flows, an organization can clearly see points of entry and exit, data interactions across systems, and interactions between users and information systems. This comprehensive view is fundamental for the assessing body to evaluate the organization's security posture accurately and determine the effectiveness of its controls in relation to CMMC requirements. While compliance checklists, employee assessment forms, and incident response plans are important tools in their own right, they do not provide the same level of clarity regarding data handling and flow as a Data Flow Diagram. Understanding how data travels within the organization is crucial for making informed decisions during an assessment, which is why the diagram is specifically highlighted as a critical tool in this context.

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://cmmcaassessor.examzify.com

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

SAMPLE