Certified Cybersecurity Maturity Model Certification (CMMC) Professional (CCP) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

Questions

1. **What is the primary role of an LPP?**
   - **A. To conduct compliance checks**
   - **B. To create CMMC approved curriculum and content**
   - **C. To evaluate C3PAOs**
   - **D. To manage practitioner registrations**

2. **What does CMMC Level 3 require in terms of documentation?**
   - **A. No documentation required**
   - **B. Limited to basic records**
   - **C. Formalizes processes and policies**
   - **D. All documentation must be publicly accessible**

3. **What does DFARS 252.204-7019 address?**
   - **A. The contractor's access to cybersecurity training**
   - **B. The notice of SPRS**
   - **C. Requirements for data encryption**
   - **D. The auditing process for compliance**

4. **How many controls are defined in CMMC Level 2?**
   - **A. 50 controls**
   - **B. 75 controls**
   - **C. 110 controls**
   - **D. 150 controls**

5. **What should occur before releasing media for reuse?**
   - **A. Updating the software on the media**
   - **B. Sanitizing or destroying information contained on the media**
   - **C. Creating backup copies of the data**
   - **D. Reviewing all user activity logs**

6. **Which of the following is a goal of the CMMC framework?**
   - **A. To ensure confidential information remains intact**
   - **B. To reduce the administrative burden on small businesses**
   - **C. To create a comprehensive federal security strategy**
   - **D. To promote transparency in financial transactions**

7. Why is it important to document Specialized and Security Protection Assets?

A. To monitor costs

B. To ensure accountability and compliance

C. For asset depreciation purposes

D. To maintain inventories alone

8. What is an LPP in the context of CMMC?

A. A Licensed Partner Provider

B. A Licensed Partner Publisher

C. A Legal Partnership Platform

D. A Liaison Partner Program

9. Who is referred to as the OSC's point of contact?

A. A senior officer of the OSC

B. The individual coordinating daily engagement

C. The primary assessor

D. The certification manager

10. Which of the following is a requirement for a Certified CMMC Professional (CCP)?

A. Must be a US citizen

B. Must have a Master's degree in information technology

C. Must have two published research papers in cybersecurity

D. Must have at least two years in cybersecurity or a related field

Answers

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

Explanations

1. What is the primary role of an LPP?

A. To conduct compliance checks

B. To create CMMC approved curriculum and content

C. To evaluate C3PAOs

D. To manage practitioner registrations

The primary role of an LPP, or Licensed Partner Publisher, is to create CMMC approved curriculum and content. LPPs are responsible for developing training materials that align with the Cybersecurity Maturity Model Certification requirements. This includes producing educational resources that support organizations in understanding and implementing the necessary practices and processes needed to achieve compliance with CMMC standards. This function is vital as the model emphasizes the importance of education and training in fostering a knowledgeable workforce capable of maintaining cybersecurity protocols. By ensuring that the curriculum is up-to-date and reflective of CMMC's evolving criteria, LPPs play a crucial part in promoting cybersecurity awareness and compliance across organizations that handle controlled unclassified information (CUI). This educational role is distinctly different from the other options as it focuses specifically on content creation rather than compliance oversight, evaluation of organizations, or administrative functions related to practitioner registrations.

2. What does CMMC Level 3 require in terms of documentation?

A. No documentation required

B. Limited to basic records

C. Formalizes processes and policies

D. All documentation must be publicly accessible

CMMC Level 3 places a strong emphasis on the formalization of processes and policies. At this level, organizations are expected to document their cybersecurity practices comprehensively to ensure that they can consistently implement these practices effectively. This documentation serves multiple purposes: it helps to establish accountability, facilitates communication among team members, supports training efforts, and prepares the organization for compliance assessments. By formalizing processes and policies, an organization demonstrates that it has a structured approach to managing and mitigating cybersecurity risks, which aligns with the objectives of the CMMC framework. The requirement for thorough documentation is essential for organizations handling Controlled Unclassified Information (CUI), as it ensures that data is protected according to specified standards and that there is a clear understanding of the procedures in place to safeguard this information. In contrast to the other options, the requirement for documentation in Level 3 is not minimal or nonexistent, nor is there an expectation for documentation to be made public. This reflects a nuanced understanding that while documentation is critical, it should not undermine the sensitive nature of the information being handled.

3. What does DFARS 252.204-7019 address?

A. The contractor's access to cybersecurity training

B. The notice of SPRS

C. Requirements for data encryption

D. The auditing process for compliance

DFARS 252.204-7019 addresses the requirement for a notice of the Supplier Performance Risk System (SPRS) within the framework of defense contracting. This clause is crucial because it mandates that contractors self-report their cybersecurity maturity levels and plans for achieving Cybersecurity Maturity Model Certification (CMMC) to the SPRS. By doing so, the Department of Defense (DoD) can assess a contractor's risk profile in relation to its cybersecurity capabilities. This reporting helps in maintaining supply chain integrity and strengthens overall cybersecurity within the defense industrial base. The other options, while relevant to cybersecurity and defense contracting, do not specifically align with the intent and content of DFARS 252.204-7019. The focus of this particular clause is on self-assessment and ensuring that the government has adequate visibility into the cybersecurity readiness of contractors.

4. How many controls are defined in CMMC Level 2?

A. 50 controls

B. 75 controls

C. 110 controls

D. 150 controls

In CMMC Level 2, there are 110 controls defined. This level serves as a stepping stone to Level 3 and consists of practices that align with the National Institute of Standards and Technology (NIST) Special Publication 800-171. Level 2 is structured to enhance an organization’s cybersecurity posture through a more comprehensive approach to implementing practices that protect sensitive information. The 110 controls encompass a variety of cybersecurity practices that organizations must implement to ensure they are prepared to handle controlled unclassified information (CUI). This level aids organizations in demonstrating their commitment to security in a more formalized manner, as they prepare for eventual compliance with Level 3, which has an even more extensive set of practices aimed at mitigating risks to sensitive data. Understanding the number of controls at each level is crucial for organizations aiming to achieve compliance, as it helps them establish a clear roadmap for improving their cybersecurity measures.

5. What should occur before releasing media for reuse?

A. Updating the software on the media

B. Sanitizing or destroying information contained on the media

C. Creating backup copies of the data

D. Reviewing all user activity logs

Before releasing media for reuse, it is crucial to sanitize or destroy any information contained on the media. This step ensures that sensitive data is permanently removed or rendered unrecoverable, thereby preventing unauthorized access or data breaches. In the context of cybersecurity best practices, proper sanitization addresses risks associated with information leakage when the media is repurposed or handed over to other users. This process can involve various methods, such as data wiping or physical destruction of the media, depending on the sensitivity of the information and organizational policies. Ensuring that all data is fully sanitized before reuse protects the confidentiality, integrity, and availability of the information and complies with data protection regulations and standards. Other considerations, such as updating software, creating backups, or reviewing user activity logs, are important in their own right but do not directly address the immediate requirement of safeguarding the information stored on the media prior to its reuse. These might be elements of overall data management and security practices, yet they do not substitute for the critical action of ensuring complete data sanitization.

6. Which of the following is a goal of the CMMC framework?

A. To ensure confidential information remains intact

B. To reduce the administrative burden on small businesses

C. To create a comprehensive federal security strategy

D. To promote transparency in financial transactions

The goal of the CMMC framework is fundamentally centered on enhancing cybersecurity practices and ensuring that sensitive information, particularly within the Department of Defense supply chain, is adequately protected. By promoting robust cybersecurity measures, the framework aims to ensure that confidential information remains intact and secure from unauthorized access and breaches. The integrity and confidentiality of sensitive data are paramount, especially in defense contracting, where the potential risks associated with cyber threats can have significant implications. The focus on protecting confidential information closely aligns with the core objectives of CMMC, which include implementing controls that not only safeguard information but also assess an organization's capability to mitigate risks associated with cybersecurity threats. The framework thus emphasizes the importance of maintaining the confidentiality, integrity, and availability of sensitive data throughout the supply chain. While ensuring confidential information remains intact is a crucial component, other choices may relate to broader goals of cybersecurity and government initiatives but do not directly reflect the primary objectives of the CMMC framework. For example, reducing the administrative burden on small businesses, while favorable, is not a specific goal of CMMC; rather, the framework aims for overall security enhancement regardless of business size. Additionally, while creating a comprehensive federal security strategy can tie into efforts surrounding cybersecurity, it is not the focal point of CMMC. Similarly, promoting

7. Why is it important to document Specialized and Security Protection Assets?

A. To monitor costs

B. To ensure accountability and compliance

C. For asset depreciation purposes

D. To maintain inventories alone

Documenting Specialized and Security Protection Assets is essential for ensuring accountability and compliance within an organization. When assets are properly documented, organizations can establish ownership, traceability, and responsibility for those assets. This accountability is crucial in meeting various regulatory requirements and standards mandated by frameworks like the CMMC. Accurate documentation also enables organizations to demonstrate compliance with security requirements, which is vital for maintaining trust with clients, stakeholders, and regulatory bodies. Additionally, proper documentation helps in the effective management of assets throughout their lifecycle, aiding in risk management and ensuring that security measures are appropriate for the types of assets involved. It provides a clear understanding of what assets are in place, their purpose, and the necessary controls to protect them against potential threats. These factors collectively contribute to a more secure and compliant operational environment.

8. What is an LPP in the context of CMMC?

A. A Licensed Partner Provider

B. A Licensed Partner Publisher

C. A Legal Partnership Platform

D. A Liaison Partner Program

In the context of CMMC, LPP stands for Licensed Partner Publisher. Licensed Partner Publishers play a critical role in the CMMC ecosystem by providing support, guidance, and educational resources to organizations striving to achieve compliance with the Cybersecurity Maturity Model Certification. They are authorized to develop and offer materials that assist in understanding the CMMC model, its requirements, and how to implement necessary practices and processes effectively. The designation as a Licensed Partner Publisher indicates that these entities have met specific qualifications and adhere to standards set by the CMMC Accreditation Body. This status empowers them to contribute to the overall knowledge and preparedness of the community in navigating the complexities of CMMC compliance, fostering an informed approach towards maintaining cybersecurity across organizations in the Defense Industrial Base. Understanding the role of Licensed Partner Publishers is crucial for organizations looking to enhance their cybersecurity posture and ensure compliance with the CMMC framework, as they serve as valuable resources for training and information dissemination.

9. Who is referred to as the OSC's point of contact?

A. A senior officer of the OSC

B. The individual coordinating daily engagement

C. The primary assessor

D. The certification manager

The point of contact for the OSC (Organization Seeking Certification) is designated as the individual coordinating daily engagement. This role is critical because it ensures effective communication and collaboration between the OSC and the various stakeholders involved in the CMMC certification process. The individual in this position is responsible for managing day-to-day interactions, scheduling meetings, sharing updates, and addressing immediate concerns that may arise during the certification journey. By being the primary facilitator of communication, this person plays a key role in ensuring that both the OSC and the assessors have the necessary information and resources to move forward efficiently. This enables a smoother process as the OSC works through the requirements of the Cybersecurity Maturity Model Certification. While other roles, such as a senior officer, primary assessor, or certification manager, may have significant responsibilities related to the certification process, they do not specifically focus on the day-to-day engagement that is critical for a successful certification experience. Each of these roles has distinct functions that contribute to the overall process, but the individual managing daily engagement is central to coordinating efforts and keeping the lines of communication open.

10. Which of the following is a requirement for a Certified CMMC Professional (CCP)?

A. Must be a US citizen

B. Must have a Master's degree in information technology

C. Must have two published research papers in cybersecurity

D. Must have at least two years in cybersecurity or a related field

The requirement for a Certified CMMC Professional (CCP) that states an individual must have at least two years of experience in cybersecurity or a related field is essential because practical experience is crucial for understanding the complexities and nuances of cybersecurity regulations and frameworks. This experience enables professionals to effectively navigate the CMMC requirements, engage with various stakeholders, and implement necessary measures to improve an organization’s cybersecurity posture. Furthermore, having real-world experience equips the CCP professional with the ability to relate theoretical knowledge to practical applications. This is particularly important in a field as dynamic and fast-evolving as cybersecurity, where the ability to adapt and apply knowledge can significantly impact assessments and compliance outcomes. Thus, practical experience not only enhances the professional's credibility but also contributes to the overall security maturity of the organizations they work with.