CCP Cyber Pro Exam Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1610 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/ccp
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1610 questions • unlimited timed mock exams • mistake book • instant explanations

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

Practice Questions

Try all 30 first, then check the answer key at the back.

1. In the context of implementing a new data access management system, what type of information must have its access permissions strictly controlled and continuously monitored?

A. Federal Contract Information
B. Publicly-Accessible Information
C. Internal Use Only Information
D. Controlled Unclassified Information

2. In the context of cybersecurity management, a company should _____ the potential cyber threats that could affect operations and _____ appropriate responses for the most critical threats.

A. Decide, dismiss
B. Acknowledge, highlight
C. Assess, formulate
D. Ignore, optimize

3. In the context of CMMC (Cybersecurity Maturity Model Certification), if BayTech is an Organization Seeking Certification (OSC) that is compliant with NIST SP 800-171, can BayTech use this compliance to assist their CMMC certification efforts?

A. Yes, CMMC certification automatically recognizes compliance with NIST SP 800-171 without additional assessment
B. No, the decision to consider NIST SP 800-171 compliance depends on the Cyber AB's discretion
C. No, CMMC certifications are distinct, and compliance with NIST SP 800-171 alone does not grant credit toward CMMC certification
D. Yes, BayTech can cite its NIST SP 800-171 compliance as evidence to support its CMMC certification

4. As the Cybersecurity Compliance Coordinator for Tech Solutions Inc., you are tasked with preparing for the CMMC assessment. Which of the following aspects should NOT be reviewed during the pre-assessment readiness check?

A. The cybersecurity posture of Tech Solutions Inc.
B. Assessment risk status
C. Logistics readiness
D. Evidence readiness

5. What is the primary purpose of the initial phase in a cybersecurity risk management effort for a small business?

A. To identify and assess potential cybersecurity threats and vulnerabilities.
B. To implement and test the effectiveness of new security controls.
C. To train employees on the business's revised security policies.
D. To monitor and review the business's incident response plan.

6. For a company seeking compliance with CMMC Level 2, which document should they refer to for establishing authentication policies? Framework Authentication Policy Source Document NIST Cybersecurity Framework NIST SP 800-63 CMMC Level 2 NIST SP 800-171R2 CMMC Level 3 NIST SP 800-53 ISO 27001 ISO/IEC 27000

A. NIST SP 800-63
B. NIST SP 800-53
C. ISO/IEC 27000
D. NIST SP 800-171R2

7. Which of the following factors does NOT typically influence the frequency of compliance reviews in a cybersecurity framework?

A. Changes in technology infrastructure
B. Past audit findings
C. The organization's annual revenue
D. Regulatory requirements

8. Incident response documentation must be structured in accordance with which framework to ensure compliance with cybersecurity standards?

A. CMMC Communication Standard
B. NIST Special Publication 800-53
C. Cybersecurity Incident Response Guidance
D. ISO 27001 Incident Standard

9. When selecting a cybersecurity tool for an organization, which of the following should not be a consideration?

A. The scalability of the tool to meet future needs
B. Personal connections of the cybersecurity team members
C. The compatibility of the tool with existing systems
D. The cost-effectiveness of integrating the tool

10. A cybersecurity team is organizing documentation for an upcoming CMMC Level 2 assessment. Based on the table below, which document type is NOT relevant to the assessment? Documentation Type Status Incident response plans Relevant Marketing materials Irrelevant Data flow diagrams Relevant System specifications for non-connected devices Irrelevant

A. Incident response plans
B. Data flow diagrams
C. System specifications for non-connected devices
D. Marketing materials

11. In developing a cybersecurity incident response plan, which elements must be included for the plan to be considered complete? Element Description 1. Identification Procedures Methods for detecting and reporting an incident 2. Roles and Responsibilities Summary of team duties and tasks 3. Communication Plans How information will be disseminated within the team and to stakeholders 4. Post-Incident Review Analysis to improve future responses 5. Routine System Diagnostics Regularly scheduled checks not tied to incident responses

A. The plan is complete with Acknowledgement Receipts from stakeholders.
B. The plan must include Identification Procedures, Roles and Responsibilities, Communication Plans, and Post-Incident Review.
C. The plan only needs Identification Procedures and Communication Plans.
D. The plan should focus on Routine System Diagnostics.

12. In which phase are network security audit findings finalized and communicated to stakeholders?

A. Report Audit Results
B. Initiate Audit
C. Conduct Risk Assessment
D. Implement Mitigation Measures

13. What term describes the mismatches between the documentation evidence of an organization's cybersecurity policies and the industry standards required for compliance?

A. Compliance gap
B. Policy deficit
C. Standard deviation
D. Documentation gap

14. During a simulated cyber incident response exercise, a facilitator must do all of the following, except:

A. Broadcast the exercise sessions to external stakeholders for feedback.
B. Ensure that all team responses are documented accurately without revealing team members' identities.
C. Debrief participants afterwards to discuss improvements while maintaining confidentiality of specific responses.
D. Verify that all recorded observations align with the cyber incident response protocols being tested.

15. In a hypothetical Cybersecurity Certification Framework, the Cyber Defense Measures category includes several elements crucial for safeguarding an organization's digital assets. Which one of the following does not belong to this category?

A. Secure Software Development Lifecycles
B. Human Resource Management Systems
C. Network Intrusion Detection Systems
D. Endpoint Protection Platforms

16. Which of the following types of data would be categorized as CUI Specified under the Cybersecurity Maturity Model Certification (CMMC) guidelines?

A. Sensitive But Unclassified (SBU)
B. Financial Information
C. Research Data
D. Trade Secrets

17. What is another name for the General Data Protection Regulation (GDPR)?

A. Digital Shield
B. Data Guardian Act
C. Privacy Protection Law
D. Cyber Security Directive

18. Which of the following are recognized cybersecurity frameworks used for assessing risk?

A. NIST Cybersecurity Framework; ISO/IEC 27001
B. NIST Cybersecurity Framework
C. ISO/IEC 27001
D. Unified Compliance Framework

19. An organization is considering updating its cybersecurity certification framework to align with modern standards. Based on the evolution from CMMC 1.0 to CMMC 2.0, what key changes should they consider? Framework Levels Maturity Processes Alignment Flexibility Features CMMC 1.0 5 Included Not fully aligned with NIST None CMMC 2.0 3 Removed Aligned with NIST SP 800-171 & 172 POAMs and waivers allowed

A. They should eliminate any alignment with national standards and focus solely on internal policies.
B. They should prioritize physical security over information security and maintain all five levels from the previous framework.
C. They should consider reducing the number of levels, removing maturity processes, and aligning with NIST standards while introducing flexibility features like POAMs and waivers.
D. They should focus on increasing the number of levels and introducing more complex assessment practices without aligning with NIST standards.

20. Ms. ABC, recently certified as a CMMC Professional, has been temporarily suspended from a board position in a non-cybersecurity organization. She is contemplating whether she needs to report this suspension to the CMMC Accreditation Body. Is Ms. ABC obligated to report her suspension, and if so, within what time frame should she make this disclosure?

A. No, there is no need to report
B. Yes, within 15 days
C. No, report only upon reinstatement
D. Yes, within 30 days

21. Manipulating data during a CMMC assessment to hide compliance failures is a violation of which of the following principles?

A. Adherence to CMMC Assessment Process
B. Confidentiality; Conflict of Interest; Adherence to CMMC Assessment Process
C. Confidentiality
D. Conflict of Interest

22. TechGuard Consulting prepared SecureIT Inc.'s systems using a checklist from the Cybersecurity Compliance Certification (CCC) framework. Later, SecureIT Inc. hired TechGuard Consulting to perform the certification assessment. Which professional standard within the CCC Code of Conduct is likely being compromised here?

A. Transparency
B. Accountability
C. Impartiality
D. Confidentiality

23. Which of the following is not a recognized principle of ethical cybersecurity practice according to the CMMC framework?

A. Accountability
B. Negligence
C. Integrity
D. Transparency

24. Jim has completed a cybersecurity training program targeting entry-level certifications. What are the next steps he should take to formalize his status as a Certified Cybersecurity Professional, aligning with industry standards?

A. Enroll in advanced courses in network security to complement his training
B. Wait for an automatic certification upgrade based on his training completion
C. Obtain his Certification Examination Code, send it to the Training Provider for validation, and successfully pass the certification exam
D. Gain at least three years of practical experience in a cybersecurity role before proceeding

25. Before assuming their role, what specific workshop must a Certified CMMC Professional (CCP) candidate attend according to organizational requirements?

A. Advanced Cyber Threats Seminar
B. CMMC Assessor Preliminary Orientation
C. Information System Security Compliance
D. Organizational Cybersecurity Compliance Workshop

26. Which of the following actions would violate the Certified CMMC Professional's Code of Professional Conduct when selecting cybersecurity software tools?

A. Evaluating tools through a transparent peer review process
B. Choosing software tools based on promises of bypassing CMMC compliance requirements
C. Selecting tools that enhance network security without unauthorized claims
D. Endorsing software that is regularly updated to meet new CMMC standards

27. Within an organization, which types of third-party vendors are most likely to have a significant impact on the company's cybersecurity compliance posture? Select all choices that apply. Vendor Type Compliance Impact Cloud service providers Significant Office supply vendors Minimal Managed security service providers (MSSP) Significant Landscaping services Minimal

A. Office supply vendors & Landscaping services
B. Cloud service providers & Managed security service providers (MSSP)
C. Office supply vendors
D. Landscaping services

28. In the pre-assessment phase for a company aiming to achieve CMMC certification, what is the first step a CMMC Professional should undertake?

A. Conduct user training sessions
B. Review recent audit logs
C. Evaluate incident response plans
D. Define the assessment scope

29. A company's network infrastructure needs to be segmented to protect sensitive customer data. Review the table below and determine the most appropriate segmentation method to prevent unauthorized access to sensitive company resources. Complete the 'Suggested Segmentation Method' for each component. Component Data Sensitivity Current Protection Measure Suggested Segmentation Method Employee Workstations Low Network Firewall Dedicated Servers High Antivirus Software Customer Database Critical Multifactor Authentication Development Environment Medium IDS

A. Intrusion Detection Systems (IDS) for Employee Workstations; Access Control Lists (ACLs) for Dedicated Servers; Network Firewall for Customer Database; Multifactor Authentication for Development Environment.
B. Security Information & Event Management (SIEM) systems for Employee Workstations; Hypervisors for Dedicated Servers; Virtual Local Area Networks (VLANs) for Customer Database; Antivirus Software for Development Environment.
C. Virtual Local Area Networks (VLANs) for Employee Workstations; Firewalls for Dedicated Servers; Access Control Lists (ACLs) for Customer Database; Hypervisors for Development Environment.
D. Remote Access Software for Employee Workstations; Antivirus Software for Dedicated Servers; Firewalls for Customer Database; VLANs for Development Environment.

30. During preparations for a data security compliance audit, the Certified CMMC Assessor (CCA) is responsible for several activities except which one?

A. Working with relevant stakeholders to establish the scope of the audit.
B. Collecting necessary documentation to support the audit process.
C. Ensuring all audit team members understand the data security requirements and procedures.
D. Granting final approval for audit outcomes and issuing compliance certificates.

Answer Key & Explanations

1. D — Controlled Unclassified Information
Controlled Unclassified Information (CUI) needs to have its access permissions strictly managed and monitored because it includes sensitive government-related information that is not classified but still requires protection. The other options listed do not have the same level of requirement for life-cycle security.

2. C — Assess, formulate
In cybersecurity management, it is essential to first assess all potential cyber threats that might impact the organization. Once the assessment is complete, the next step is to formulate appropriate response strategies for the threats identified as most critical, ensuring resources are allocated effectively to manage these risks.

3. C — No, CMMC certifications are distinct, and compliance with NIST SP 800-171 alone does not grant credit toward CMMC certification
Compliance with NIST SP 800-171 is not automatically accepted in the CMMC certification process. Each certification path must meet the distinct criteria required by CMMC levels, and external frameworks like NIST SP 800-171 do not automatically translate into CMMC compliance without official recognition or policy allowing for such credit.

4. A — The cybersecurity posture of Tech Solutions Inc.
The pre-assessment readiness check for a CMMC assessment involves reviewing aspects such as the assessment risk status, logistics readiness, and evidence readiness. The cybersecurity posture of the organization is assessed during the actual CMMC assessment, not during the readiness review.

5. A — To identify and assess potential cybersecurity threats and vulnerabilities.
The initial phase in a cybersecurity risk management effort focuses on identifying and assessing potential cybersecurity threats and vulnerabilities to understand what needs to be addressed to protect the business effectively.

6. D — NIST SP 800-171R2
For organizations adhering to CMMC Level 2, NIST SP 800-171R2 provides the necessary guidelines for setting up authentication policies, thus aligning the cybersecurity practices with the required standards.

7. C — The organization's annual revenue
While regulatory requirements, changes in technology infrastructure, and past audit findings can directly influence the frequency of compliance reviews, an organization's annual revenue is generally not a direct factor in determining how often compliance checks are performed.

8. C — Cybersecurity Incident Response Guidance
The correct structuring and alignment of incident response documentation is essential for maintaining cybersecurity compliance. In this context, the Cybersecurity Incident Response Guidance provides the appropriate framework to follow, ensuring all procedural documentation aligns with cybersecurity standards.

9. B — Personal connections of the cybersecurity team members
When selecting a cybersecurity tool, considerations should primarily focus on technical compatibility, cost, and scalability to meet future business needs. Personal connections should not influence technical decision-making, as this could lead to biases and potential security risks.

10. D — Marketing materials
Marketing materials are not relevant to a CMMC Level 2 assessment. The assessment focuses on cybersecurity policies, procedures, and data flow diagrams to ensure adequate security measures are in place.

11. B — The plan must include Identification Procedures, Roles and Responsibilities, Communication Plans, and Post-Incident Review.
For an incident response plan to be considered complete, it must address core components including methods for incident detection and reporting, defined roles and responsibilities, effective communication plans, and post-incident review procedures.

12. A — Report Audit Results
In the 'Report Audit Results' phase, the finalized audit findings are formally communicated to stakeholders. Before this, audit initiation, risk assessment, and mitigation implementation occur, but they do not involve finalizing or communicating results.

13. D — Documentation gap
A documentation gap identifies the disparity between what is stated in a company's cybersecurity policy documentation and what is actually required by industry standards for full compliance.

14. A — Broadcast the exercise sessions to external stakeholders for feedback.
During a simulated cyber incident response exercise, it is crucial to maintain the confidentiality of participants' strategies and identities, and sharing such sessions with external parties could compromise this confidentiality.

15. B — Human Resource Management Systems
The Cyber Defense Measures category focuses on technical solutions aimed at protecting digital infrastructure, like Network Intrusion Detection Systems, Endpoint Protection Platforms, and Secure Software Development Lifecycles. Human Resource Management Systems are not typically included in technical cybersecurity measures.

16. A — Sensitive But Unclassified (SBU)
CUI Specified is a subset of Controlled Unclassified Information (CUI) that has specific handling requirements. Sensitive But Unclassified (SBU) is categorized as CUI Specified because it requires particular safeguarding measures mandated by law, regulation, or government policy.

17. A — Digital Shield
The General Data Protection Regulation (GDPR) is often known as the "Digital Shield" because it serves as a comprehensive framework for protecting personal data and privacy in the European Union. It provides individuals with greater control over their personal information and places stringent obligations on organizations handling such data.

18. A — NIST Cybersecurity Framework; ISO/IEC 27001
Recognized cybersecurity frameworks include the NIST Cybersecurity Framework and ISO/IEC 27001, both

of which provide guidelines for risk management in information security. The Unified Compliance Framework is not specifically a risk assessment framework, but rather a tool that helps organizations comply with multiple regulations and frameworks.

19. C — They should consider reducing the number of levels, removing maturity processes, and aligning with NIST standards while introducing flexibility features like POAMs and waivers.
The organization should streamline practices by reducing the number of certification levels, removing maturity processes, and aligning their standards with NIST SP 800-171 & 172. Additionally, they should allow for flexibility with time-limited POAMs and waivers, similar to the transition from CMMC 1.0 to CMMC 2.0.

20. D — Yes, within 30 days
Ms. ABC is required to report her suspension to the CMMC Accreditation Body as it reflects on professional conduct which is under the purview of their monitoring, regardless of whether it directly involves cybersecurity roles. The report has to be made within 30 days to comply with CMMC guidelines.

21. B — Confidentiality; Conflict of Interest; Adherence to CMMC Assessment Process
Manipulating data to conceal compliance failures undermines the principles of confidentiality, introduces a conflict of interest, and goes against the adherence to the CMMC assessment process. These actions can compromise the integrity and credibility of the certification process.

22. C — Impartiality
According to professional standards in cybersecurity assessments, entities conducting assessments should remain impartial. Having the same entity assess the effectiveness of practices it helped implement creates a conflict of interest and affects impartiality.

23. B — Negligence
Negligence is not a recognized principle of ethical cybersecurity practice. The CMMC framework emphasizes the need for integrity, transparency, and accountability to maintain trust and ensure effective security measures.

24. C — Obtain his Certification Examination Code, send it to the Training Provider for validation, and successfully pass the certification exam
To become certified, Jim needs to obtain a Certification Examination Code, send this code to the Training Provider to prove his program completion, and then pass the certification exam. Practical experience and further courses, while beneficial, are not required to achieve the entry-level certification.

25. D — Organizational Cybersecurity Compliance Workshop
A CCP candidate must complete the "Organizational Cybersecurity Compliance Workshop" to meet their organization's specific training prerequisites before assuming their role.

26. B — Choosing software tools based on promises of bypassing CMMC compliance requirements
The Code of Professional Conduct for Certified CMMC Professionals prohibits any endorsement or selection of tools based on unauthorized claims that circumvent official compliance processes. This ensures that all aspects of cybersecurity practices adhere to the established standards without shortcuts or unethical promises.

27. B — Cloud service providers & Managed security service providers (MSSP)
Third-party vendors like cloud service providers and MSSPs often have access to critical data and systems, directly impacting cybersecurity compliance.

28. D — Define the assessment scope
The initial step in the pre-assessment phase is to define the assessment scope. This involves understanding what parts of the organization and processes will be evaluated against the CMMC requirements. Other tasks, such as user training or reviewing audit logs, are important but come later in the process.

29. C — Virtual Local Area Networks (VLANs) for Employee Workstations; Firewalls for Dedicated Servers; Access Control Lists (ACLs) for Customer Database; Hypervisors for Development Environment.
Segmenting network infrastructure is crucial to protecting sensitive data. VLANs help separate workstation traffic. Dedicated servers benefit from firewalls to control access. ACLs manage who can access the customer database. Hypervisors isolate development environments.

30. D — Granting final approval for audit outcomes and issuing compliance certificates.
The CCA is responsible for overseeing the preparation phase, including defining scope, gathering relevant documentation, and ensuring team readiness. However, the final approval for audit outcomes and issuing compliance certificates is not typically within the CCA's responsibilities; this is typically handled by other authorities within the organization or certification body.

Ready to pass?

Unlock the full CCP Cyber Pro Exam Prep bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/ccp

Watch the full video walkthrough on YouTube @CertsQuizPrep