





Preparing for Your CMMC Interview: Commonly Asked Questions – Physical Protection Edition

Picture a bank with security guards and a vault, or a castle with a moat and drawbridge. These physical barriers ensure that the actual systems, devices, and storage locations for sensitive information are physically secure. The focus is on implementing tangible measures to prevent unauthorized physical access to facilities, equipment, and other resources as well as, protecting against environmental hazards. This may be implemented through a variety of protective measures, including security guards, visitor control desks, CCTV cameras, badge readers, secured server/storage rooms, and more.

Key

-  Domain Family
-  Identifier
-  Basic | Derived
-  Security Requirement

Security Requirement Table of Contents

Physical Protection

- Enforce safeguarding measures for CUI at alternate work sites.....4
- Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.....5
- Protect and monitor the physical facility and support infrastructure for organizational systems.....6
- Escort visitors and monitor visitor activity.....7
- Maintain audit logs of physical access.....8
- Control and manage physical access devices.....9

As you prepare for your organization’s assessment, it’s important to understand what to expect during the interview process. Individuals can anticipate a range of questions that will be both comprehensive and reflective of several key areas intended to assure that the controls are implemented correctly and performing as expected. Interview sessions typically follow a basic pattern to help inform this decision. Below is an example interview session construct. Though not all inclusive these guides provide typical questions asked during an assessment.

Typical Question Format:

Policy and Procedures:

- How does your organization’s security policy address the encryption of Controlled Unclassified Information (CUI) on mobile devices and platforms?
- Can you provide documentation or guidelines that mandate encryption on mobile devices and platforms when handling CUI?

Implementation:

- What encryption standards or protocols does your organization use for CUI on mobile devices?
- Are there specific mobile device management (MDM) or mobile application management (MAM) tools in place to enforce encryption on mobile devices and platforms?
- How do you ensure that all mobile devices used within the organization have encryption enabled?

Monitoring and Auditing:

- How do you monitor and verify that CUI remains encrypted on mobile devices and platforms?
- Are there any auditing mechanisms in place to check for devices that might have encryption disabled or bypassed?
- Can you provide recent audit logs or reports showing encryption checks for mobile devices?

Incident Handling:

- Have there been any incidents where CUI was found unencrypted on a mobile device? If so, how was it handled?
- What are the consequences or actions taken against users who fail to encrypt CUI on their mobile devices?

Training and Awareness:

- How are employees made aware of the importance of encrypting CUI on mobile devices?
- Is there a specific training module or awareness campaign focused on mobile device encryption?

Technical:

- Can you demonstrate the encryption settings on a sample mobile device used within the organization?
- Are there any exceptions or scenarios where CUI might not be encrypted on mobile devices, and how are these exceptions handled?

Third-party and BYOD:

- How does your organization ensure that third-party vendors or contractors adhere to this encryption requirement when accessing CUI on mobile devices?
- If you have a Bring Your Own Device (BYOD) policy, how do you ensure that personal devices encrypt CUI?



Physical Protection

PE.L2-3.10.6

Derived

Enforce safeguarding measures for CUI at alternate work sites.

- How does your organization define and identify alternate work sites?
- What specific safeguarding measures are implemented for CUI when accessed or processed at alternate work sites?
- How do you ensure employees are aware of and adhere to CUI safeguarding measures when working remotely or off-site?
- Are there specific tools or technologies in place to secure CUI when accessed from alternate locations?
- How do you monitor and log access to CUI from off-site locations?
- How do you handle the secure transmission of CUI between primary and alternate work sites?
- What measures are in place to prevent unauthorized access or disclosure of CUI at alternate work sites?
- How do you ensure the physical security of devices or materials containing CUI at off-site locations?
- Are there specific training programs or guidelines provided to employees about managing CUI at alternate work sites?
- How do you manage and secure CUI on portable devices such as laptops or USB drives?
- What incident response measures are in place for potential breaches or unauthorized access to CUI at alternate sites?
- How frequently do you review and update policies related to safeguarding CUI at off-site locations?
- How do you handle situations where third-party vendors or partners access CUI from alternate work sites?
- Are there periodic security audits or checks for devices or locations involved in off-site CUI processing?
- How do you ensure encrypted storage and transmission of CUI when accessed from remote or alternate sites?
- How do you verify the security posture of alternate work sites, especially if they are personal or home environments?
- How do you manage feedback or concerns from employees regarding the safeguarding of CUI at off-site locations?
- Are there specific controls or restrictions on the types of CUI that can be accessed or processed at alternate work sites?
- How do you collaborate with other entities or industry peers to stay updated on best practices for safeguarding CUI at off-site locations?
- How do you ensure that your approach to safeguarding CUI at alternate work sites aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection

PE.L1-3.10.1

Basic

Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

- How do you control physical access to your organizational systems and equipment?
- What authentication mechanisms (e.g., access cards, biometrics) are in place to ensure only authorized individuals gain physical access?
- Describe the process for authorizing individuals to have physical access to specific areas or equipment.
- How do you track and log physical access to sensitive areas where systems and equipment are housed?
- How frequently is the list of individuals with authorized physical access reviewed and updated?
- Are there security personnel or surveillance systems in place to monitor and enforce physical access controls?
- How do you handle visitors or third-party contractors who require temporary physical access?
- Describe the protocols in place for quickly revoking physical access when an individual's authorization is terminated or changed.
- How do you ensure that physical access controls are maintained during emergencies or special circumstances?
- What measures are in place to detect and respond to unauthorized physical access attempts?
- How do you integrate physical access controls with other security systems or protocols, such as intrusion detection systems?
- How do you handle physical access controls in remote or secondary facilities, if applicable?
- Describe any challenges or incidents related to unauthorized physical access and how they were addressed.
- How do you educate and train relevant personnel about the importance of and procedures for physical access controls?
- Are there periodic security drills or simulations to test the effectiveness of physical access controls?
- How do you stay updated on best practices and industry standards related to physical access control?
- Are backup or redundant power supplies in place to ensure access control mechanisms remain operational during power outages?
- Are there periodic security audits or assessments to validate the adherence to and effectiveness of physical access controls?
- How do you ensure that physical security measures don't inadvertently hamper legitimate business operations or emergency responses?

- How do you ensure that the approach to controlling physical access aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection



PE.L2-3.10.2



Basic



Protect and monitor the physical facility and support infrastructure for organizational systems.

- How do you ensure the physical security of facilities housing your organizational systems?
- What access control measures are in place for these facilities?
- Describe the surveillance or monitoring systems deployed at these facilities.
- How do you manage and track authorized personnel access to these facilities?
- What measures are in place to detect and respond to unauthorized access or breaches in the physical facility?
- How do you protect the supporting infrastructure, such as power supplies, cooling systems, and network connections?
- Are there automated alerts or systems in place to notify of any disruptions or issues in the support infrastructure?
- How frequently do you review and test the physical security measures in place?
- Describe any backup or redundancy systems in place for critical infrastructure components.
- How do you handle third-party or vendor access to the physical facilities?
- What training or awareness programs are in place to ensure staff understand and adhere to physical security protocols?
- How do you integrate physical security with other security and incident response systems?
- Describe any challenges or issues you've encountered related to physical facility security and how they were addressed.
- How do you ensure continuous monitoring and protection of facilities in the event of emergencies or natural disasters?
- Are there periodic drills or exercises to test the effectiveness and readiness of physical security measures?
- How do you handle the disposal or decommissioning of equipment to ensure data security within the facility?
- How do you manage and secure remote or secondary facilities, if applicable?

- How do you stay updated on best practices and industry standards related to physical security and infrastructure protection?
- Are there periodic security audits or assessments to validate the effectiveness of your physical facility protection measures?
- How do you ensure that the approach to protecting and monitoring physical facilities and infrastructure aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection



PE.L1-3.10.3



Derived



Escort visitors and monitor visitor activity.

- How does your organization manage and control physical access for visitors?
- What procedures are in place to ensure visitors are escorted at all times while in secure or sensitive areas?
- How do you verify the identity of visitors before granting them access?
- What training or guidelines are provided to staff responsible for escorting visitors?
- Describe the mechanisms or tools used to monitor visitor activity during their stay.
- How are visitors made aware of the organization's security policies and their responsibilities while on-site?
- How do you handle visitors who need access to sensitive or restricted areas?
- Are there specific protocols or requirements for visitors from foreign entities or third-party vendors?
- How do you ensure that visitors don't inadvertently access or view sensitive information or systems?
- What processes are in place for logging visitor entries, exits, and their activities during the visit?
- How frequently are visitor logs reviewed, and by whom?
- Are there automated systems or surveillance tools in place to assist with monitoring visitor activity?
- How do you manage and respond to any security incidents or policy violations involving visitors?
- Describe any challenges or issues you've encountered related to escorting or monitoring visitors and how they were addressed.
- Are there periodic drills or assessments to test the effectiveness of your visitor management protocols?
- How do you ensure that visitor management procedures don't interfere with business operations or events?

- How do you handle scenarios where visitors require repeated or prolonged access, such as contractors or consultants?
- Are there specific protocols for managing visitor access during emergencies or special events?
- How do you gather feedback or concerns from staff and visitors related to the visitor management process?
- How do you ensure that your approach to escorting and monitoring visitors aligns with NIST guidelines and broader security objectives?



Physical Protection

PE.L1-3.10.4

Derived

Maintain audit logs of physical access.

- How does your organization log physical access events to your facilities or secure areas?
- What tools or systems are used to capture and store these physical access logs?
- How long are physical access logs retained, and where are they stored?
- What specific details or data points are captured in the physical access logs?
- How frequently are the physical access logs reviewed, and by whom?
- Are there automated alerts set up for unauthorized or suspicious physical access attempts?
- How do you ensure the integrity and confidentiality of the physical access logs?
- Describe the process for granting and revoking physical access permissions to different areas of your facility.
- How do you handle physical access logging for temporary or guest visitors?
- What measures are in place to ensure that physical access logs are complete and not tampered with?
- How are physical access logs integrated with other security systems or incident response protocols?
- How do you manage and audit third-party or vendor physical access to your facilities?
- Describe any challenges or issues you've encountered related to physical access logging and how they were addressed.
- How do you ensure that physical access logs are compliant with data protection or privacy regulations?
- Are there periodic security audits or assessments to validate the comprehensiveness and accuracy of your physical access logs?
- How do you handle the disposal or archiving of older physical access logs?

- How do you train security personnel or staff responsible for managing and reviewing physical access logs?
- How do you address discrepancies or anomalies detected in the physical access logs?
- How do you stay updated on best practices and industry standards related to physical access logging?
- How do you ensure that the approach to maintaining physical access audit logs aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection



:E.L1-3.10.5



Derived



Control and manage physical access devices.

- What types of physical access devices does your organization use (e.g., key cards, biometric scanners, RFID tags)?
- How do you ensure the security and integrity of these physical access devices?
- Describe the process for issuing, activating, and deactivating physical access devices.
- How do you track and monitor the use of physical access devices across your facilities?
- What measures are in place to prevent cloning, tampering, or unauthorized use of physical access devices?
- How frequently do you audit the usage logs of physical access devices?
- How do you handle lost, stolen, or compromised physical access devices?
- Are there automated alerts or mechanisms to detect suspicious or anomalous activity related to physical access devices?
- How do you integrate physical access device controls with other security systems, such as surveillance cameras or intrusion detection systems?
- Describe the process for updating or upgrading the technology or security features of physical access devices.
- How do you manage and control visitor or temporary physical access devices?
- What training or awareness programs are in place for employees regarding the proper use and security of physical access devices?
- How do you ensure redundancy or backup access mechanisms in case of failure or malfunction of primary physical access devices?
- Describe any challenges or issues you've faced related to managing physical access devices and how they were addressed.

- Are there specific protocols for the use of physical access devices in high-security areas or sensitive locations within your facilities?
- How do you handle the decommissioning or disposal of outdated or unused physical access devices?
- How do you verify the authenticity and security of third-party or externally sourced physical access devices?
- How do you stay updated on industry best practices and emerging threats related to physical access devices?
- Are there periodic security reviews or tests to validate the effectiveness and security of your physical access devices?
- How do you ensure that the management and control of physical access devices align with NIST guidelines and your organization's broader cybersecurity objectives?

WHY REDSPIN

- Over 100 security advisors and assessors, ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including multiple Joint Surveillance Voluntary Assessment Program (JSVAP) assessments
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified



Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.



40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com