Cyber AB CCA - Quiz Questions with Answers

Assessing CMMC Level 2 Practices

1.

Any user that accesses CUI on system media should be authorized and have a lawful business purpose. While assessing a contractor?s implementation of MP.L2-3.8.2-Media Access, you examine the CUI access logs and the role of employees. Something catches your eye where an ID of an employee listed as terminated regularly accesses CUI remotely. Walking into the contractor?s facilities, you observe the janitor cleaning an office where documents marked CUI are visible on the table. Interviewing the organization?s data custodian, they informed me that a media storage procedure is augmented by a physical protection and access control policy. Based on the scenario and the requirements of CMMC practice MP.L2-3.8.2-Media Access, which of the following actions would be the highest priority recommendation for the contractor?

Develop and implement a process for timely disabling or revoking access to CUI upon employee termination.

Invest in more sophisticated access control technology for their systems.

Implement a system for logging and monitoring all access attempts to CUI resources.

Conduct additional training for employees on handling CUI materials.

Developing and implementing a process for timely disabling or revoking access to CUI upon employee termination directly addresses the critical security gap identified in the scenario. It is a high-priority action to ensure access to CUI is limited to authorized users.

2.

You decide to interview the IT security team to understand if and how a contractor has implemented audit failure alerting. You learn they have deployed AlienVault OSSIM, a feature-rich security information and event management (SIEM) tool. The SIEM tool has been configured to send automatic alerts to system and network administrators if an event affects the audit logging process. Alerts are generated for the defined events that lead to failure in audit logging and can be found in the notification section of the SIEM portal. However, the alerts are sent to the specified personnel 24 hours after the occurrence of an event. For the implementation of CMMC practices, how would you score AU.L2-3.3.4-Audit Failure Alerting?

Not Met

Fully Met

Not Applicable

Partially Met

Even though the contractor has implemented some aspects like identifying personnel, defining event types[a], and having an alerting mechanism, the significant delay fails to fully satisfy the intent of timely alerting for audit logging failures. The Further Discussion part of AU.L2-3.3.4-Audit Failure Alerting requires the contractor's designated security personnel to be aware when the audit log process fails or becomes unavailable. The contractor's configuration of the SIEM to send notifications after 24 hours defeats the purpose of implementing the practice in the first place. If security personnel are unaware of the audit logging process failure, then any suspicious or malicious activities can arise within 24 hours without their knowledge. Thus, despite the contractors' efforts, the practice will be scored as Not Met.

3.

When examining an OSC?s procedures for addressing transmission integrity and confidentiality, you interview their system administrator and learn that they use Secure File Transfer Protocol (SFTP) for secure CUI transmission. The OSC employs AES-256 to encrypt data before transmitting it. Any external connections to their internal servers or systems can only occur via a VPN. All emails containing CUI are encrypted and sent using Secure/Multipurpose Internet Mail Extensions (S/MIME). Internal CUI transfers are conducted over WPA3 secure Wi-Fi. All areas of the OSC?s facilities where CUI is stored or processed are secured with biometrics. To prevent unauthorized CUI exfiltration or transfer, the OSC has deployed a data loss prevention solution. During employee interviews, you learn they receive regular awareness training on the importance of data encryption during transmission. Additionally, they conduct regular audits of transmission protocols and encryption measures to ensure their effectiveness. While WPA3 offers improved security compared to previous versions, what additional control measure could further enhance the protection of CUI on the Wi-Fi network, specifically focusing on data in transit?

Segmenting the Wi-Fi network to isolate CUI-related traffic from other types network activity.

Implementing a guest network that restricts access to non-essential devices.

Enforcing stricter password complexity requirements for Wi-Fi access.

Disabling unused Wi-Fi access points within the facility to reduce attack surfaces.

By isolating CUI-related traffic on a separate Wi-Fi segment, the OSC can minimize the potential for unauthorized access or eavesdropping on data in transit within the internal network.

4.

An OSC has an established Incident Response plan and a dedicated team specifically trained to handle any potential incidents and conduct necessary analysis. When performing the assessments, you also realize the OSC has deployed IDS and SIEM tools to identify possible incidents. Examining the Contractor's incident response policy, you also learn they have defined and implemented containment strategies and have developed clear procedures for system and data recovery after an incident, including backup and restore procedures. There is also a communication protocol in place to inform the affected stakeholders and users after a security incident. Chatting with a few members of the OSC's incident response team, you learn they conduct regular drills to test and improve the effectiveness of the incident-handling capability. There also are defined and documented incident response mechanisms and a post incident analysis procedure to identify lessons learned and make necessary improvements to the incident-handling process. If a subcontractor or contractor discovers malware connected to an incident when assessing the impact of the incident, what should they do?

Quarantine and submit the malware to the DoD Cyber Crime Center (DC3)

Send the malware to the contracting officer

Delete everything affected by the malware

Quarantine and send the malware to their CISO

According to DFARS 252.204-7012, when a contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, they should submit the malicious software to the DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Under the clause, sending malicious software to the Contracting Officer is prohibited.

5.

A Defense Contractor is a CMMC Level 2 organization that frequently needs to transport digital media containing CUI between their main office and an off-site data storage facility. In preparing for their upcoming CMMC assessment, the organization's OSC has closely reviewed the requirements of CMMC practice MP.L2-3.8.6-Portable Storage Encryption, which specifically addresses the protection of CUI stored on digital devices during transport. The OSC recognizes that their current practices of simply placing the media in standard packaging and using commercial shipping services do not fully meet the control's mandatory requirements. Under CMMC practice MP.L2-3.8.6-Portable Storage Encryption, what is the mandatory requirement to protect CUI stored on digital devices during transport? Under CMMC practice MP.L2-3.8.6-Portable Storage Encryption, what is the mandatory requirement to protect CUI stored on digital devices during transport?

To protect its confidentiality by encrypting it using FIPS 140-2 compliant cryptographic modules

To ensure it is safeguarded by trained guards and transported using a reputable shipping company

To never transport CUI outside the controlled environment

To store CUI only on self-destructing media that erases data if tampered with.

CUI can be stored and transported on a variety of portable media, which increases the chance that the CUI can be lost. When identifying the paths CUI flows the OSC must also identify devices to include in this practice. To mitigate the risk of losing or exposing CUI, CMMC practice MP.L2-3.8.6-Portable Storage Encryption mandates OSCs to implement an encryption scheme to protect the data. This way, even if the media is lost, proper encryption renders the data inaccessible. When encryption is not an option, apply alternative physical safeguards during transport.

6.

You are the lead CMMC assessor evaluating a defense contractor that develops advanced surveillance equipment and software for intelligence agencies. Given the sensitive nature of their work, the contractor has implemented robust insider threat monitoring. During your assessment, you find out that the contractor's insider threat program tracks indicators like unauthorized data access attempts, unexplained wealth changes, workplace disputes, and disruptive behavior changes. The contractor also has regular security awareness training covering reporting potential insider threats via an anonymous hotline and web portal. High-risk roles like developers with classified codebase access receive additional insider threat vector training and are closely monitored. To verify all this, you interview the CISO, who confirms their implementation of CMMC practice AT.L2-3.2.3-Insider Threat Awareness. Your assessment reveals the contractor's insider threat monitoring system generates alerts based on a pre-defined set of thresholds. However, some security experts recommend a risk-based approach. What is the primary advantage of a risk-based approach to insider threat detection?

A risk-based approach prioritizes alerts based on the potential severity from the threat.

It reduces the overall number of alerts generated.

It eliminates the need for human intervention in the monitoring process.

It simplifies the training required for security personnel.

The primary advantage of a risk-based approach to insider threat detection is that it allows organizations to prioritize their resources and efforts on the most significant and likely threats, thereby increasing the efficiency and effectiveness of their security measures. A risk-based approach enables organizations to identify and concentrate on the highest-risk individuals, activities, or assets, rather than treating all potential insider threats equally. This prioritization ensures that limited resources, such as time, personnel, and technology, are allocated where they are most needed and can have the greatest impact. It also makes the process more efficient by letting lower-risk activities be monitored passively.

7.

Upon examining a contractor's Security and awareness training policy for compliance with AT.L2-3.2.2-Role-Based Training, you determine that they offer their employees training on handling CUI securely. However, system auditors, system administrators, penetration testers, and other cybersecurity roles are all provided biannual training on CUI handling and cybersecurity best practices. During your assessment, you reviewed their training materials and curriculum for network engineers. You found that the training covers basic networking concepts and doesn't delve into secure network configuration practices or identify potential network security risks. Which of the following best describes the likely outcome of this finding in your assessment report?

The lack of specific training for network engineers would likely result in a finding of non-compliance with AT.L2-3.2.2-Role-Based Training.

The finding does not impact the assessment, as network security is not a CMMC requirement

The assessment will be postponed until the contractor revises all training materials for all roles.

The finding might be documented as an observation for improvement but wouldn't affect the overall compliance score.

The scenario describes a gap in role-based training for network engineers. CMMC practice AT.L2-3.2.2--Role-Based Training requires personnel to be trained to carry out their information security duties effectively. This gap would likely be documented as a non-compliance finding.

8.

You are evaluating an OSC for compliance with CMMC Level 2 practices. During your assessment of SC controls, you use a series of assessment methods to understand how effectively the OSC has implemented them. The OSC has a documented security policy outlining user roles and responsibilities. The OSC?s system and communications protection policy states that basic user and privileged functionalities are separated. They have deployed Azure AD to help enforce this requirement through identity management. Interviews with system administrators reveal they have elevated privileges for system management tasks. A review of system configuration settings shows separate user accounts for standard users and administrators. However, you notice that some employees use personal cloud storage services for storing work documents. Which of the following assessment methods would be most helpful in gathering additional evidence regarding the OSC?s compliance with CMMC practice SC.L2-3.13.4-Shared Resource Control?

Examining the OSC?s acceptable use policy (AUP) for restrictions on cloud storage usage.

Reviewing interview transcripts with system developers.

Analyzing network traffic logs for suspicious data transfer activity.

Testing system configurations related to data encryption at rest.

The OSC?s acceptable use policy (AUP) is the most likely document to outline restrictions on shared resources, including cloud storage services. CMMC practice SC.L2-3.13.4-Shared Resource Control focuses on preventing unauthorized information transfer through shared resources, and the AUP should detail the organization?s controls to achieve this objective. Reviewing the AUP would provide direct evidence of the OSC?s approach to managing shared resources and any potential limitations on personal cloud storage usage.

9.

An OSC uses VoIP from a reputable vendor for video conferencing with external partners. They have a documented policy outlining authorized users and approved platforms for video conferencing. All VoIP traffic is encrypted to protect the content of the communication from interception and eavesdropping. The security team has deployed a firewall and an Intrusion Detection and Prevention System (IDPS) specifically for the VoIP system. When interviewing the communications team about access controls, you learn that users receive an autogenerated link to enter the conference upon clicking. The team also monitors the system daily to ensure that any malicious activities are detected and addressed according to their incident response plan. From a CMMC compliance perspective with SC.L2-3.13.14-Voice over Internet Protocol, which aspect of the organization's video conferencing setup raises the most concern regarding the control of VoIP usage?

Encryption protects the content of communication, but user access control is not addressed.

The documented policy outlines authorized users and platforms, which is good practice.

A firewall and Intrusion Detection and Prevention System (IDPS) are deployed for the VoIP system, providing network protection.

Using a reputable VoIP vendor ensures a secure platform.

SC.L2-3.13.14-Voice over Internet Protocol, [a] emphasizes controlling VoIP usage. While other measures highlight security aspects, the primary concern is user access control. Relying solely on auto-generated links for access might not ensure user authentication, potentially allowing unauthorized individuals to join conferences if they obtain a link.

10.

A vulnerability scan on a defense contractor's system identifies a critical security flaw in a legacy database application that stores CUI. Remediating the flaw would require a complete overhaul of the application, causing significant downtime and potentially disrupting critical business functions. Given the potential consequences of remediation, the contractor is considering deferring the fix. Which course of action best aligns with the guidance of CMMC practice RA.L2-3.11.3-Vulnerability Remediation?

Document the risk acceptance rationale and continue monitoring the risk from the vulnerability

Permanently disregard the vulnerability and take no further action

Implement compensating controls to reduce the associated risk

Immediately contract a third party to assist with remediation

---

CMMC practice RA.L2-3.11.3-Vulnerability Remediation, requires action to be taken for remediation, acceptance, avoidance or transference. If a vulnerability cannot be remediated then the organization needs to accept the risk and make a risk-based decision. To do this, the OSC must document the vulnerability, acknowlegde they are accepting the risk, along with the rationale for risk acceptance, and ensure the risk from the unmitigated vulnerability is monitored continuously in case risk factors change.

11.

You decide to interview the IT security team to understand if and how a contractor has implemented audit failure alerting. You learn they have deployed AlienVault OSSIM, a feature-rich security information and event management (SIEM) tool. The SIEM tool has been configured to send automatic alerts to system and network administrators if an event affects the audit logging process. Alerts are generated for the defined events that lead to failure in audit logging and can be found in the notification section of the SIEM portal. However, the alerts are sent to the specified personnel 24 hours after the occurrence of an event. As an assessor evaluating the implementation of AU.L2-3.3.4-Audit Failure Alerting, which of the following would be a key consideration regarding the evidence provided by the contractor?

Verifying that the types of audit logging failures defined cover a comprehensive range of potential scenarios

Ensuring the defined alert notification methods (e.g., email, SMS) are secure and encrypted

Determining if the documented personnel roles for alert notification align with the organization's hierarchy

Checking if the alert notification process integrates with third-party monitoring services

---

When assessing the sufficiency and adequacy of a contractor's implementation of AU.L2-3.3.4-Audit Failure Alerting, a key consideration should be verifying that the types of audit logging failures defined cover a comprehensive range of potential scenarios. Per CMMC guidance, practice AU.L2-3.3.4 requires defining the "types of audit logging process failures for which alerts will be generated." An assessor should review the contractor's documentation to ensure they have identified a sufficiently broad range of failure scenarios, including software errors, hardware failures, storage capacity issues, component-level failures, and overall system/centralized logging solution failures. Comprehensively defining these failure types is crucial to ensure appropriate alerting mechanisms are in place to effectively detect and respond to various audit logging process failures. The other options, while relevant to the practice, may not be the primary focus areas for an assessor evaluating the sufficiency and adequacy of the implementation evidence provided by the contractor.

12.

An OSC has documented HR and personnel security policies, which are well integrated. A key requirement is that credentials and systems are revoked upon a transfer or termination. Their personnel security policy includes procedures for transfer and termination, a list of system accounts tied to each employee, and management of revoked or terminated credentials and authenticators. Examining the procedures addressing personnel transfer and termination, you learn that besides revoking or terminating system access, authenticators, and credentials, the OSC recovers all company IT equipment, access/identification cards, and keys from the transferred or terminated employee. They also interview the employee to remind them of their CUI handling obligations even after transfer and require them to sign an NDA. After every termination, they also change the password and other access control mechanisms and notify all the stakeholders that the employee has been terminated or transferred. After personnel termination or transfer, the OSC should do all the following, EXCEPT? Choose all that apply.

Keep tabs on the terminated employee to ensure they do not sell company secrets or disseminate CUI

Notify stakeholders that an employee has been terminated and is no longer associated with the company.

Change passwords and shared keys to which a transferring or departing individual had access.

Implement continuous monitoring to detect any unauthorized access attempts after personnel changes.

CMMC practice PS.L2-3.9.2-Personnel Actions, focuses on revoking access, retrieving equipment, conducting exit interviews, and notifying stakeholders upon personnel termination or transfer. Although not explicitly mentioned, monitoring information systems after personnel changes is necessary to ensure any attempts to use old credentials and authenticators to access information systems are detected. However, spying on or keeping tabs on terminated employees may infringe on their privacy and is not recommended.

13.

A contractor has retained you to assess compliance with CMMC practices as part of their triennial review. During your assessment of the AU domain, you discovered that the contractor has recently installed new nodes and servers on their network infrastructure. To assess their implementation of AU.L2-3.3.7-Authoritative Time Source, you trigger some events documented to meet AU.L2-3.3.1-System Auditing across both the new and existing systems, generating audit logs. Upon examining these logs, you notice inconsistencies in the time stamps between newly installed and previously existing nodes. Further investigation reveals that while the contractor has implemented a central Network Time Protocol (NTP) server as the authoritative time source, the new systems are configured to automatically adjust and synchronize their clocks only when the time difference with the NTP server exceeds 30 seconds. How would you assess the contractor's implementation of AU.L2-3.3.7-Authoritative Time Source?

Not Met

Met

Not Applicable

Partially Met

The CMMC practice AU.L2-3.3.7-Authoritative Time Source requires that "internal system clocks used to generate time stamps for audit records are compared to and synchronized with an authoritative time source." While the contractor has implemented a central NTP server as the authoritative time source, the fact that the new systems are configured to automatically adjust and synchronize their clocks only when the time difference with the NTP server exceeds 30 seconds does not meet the requirement for consistent synchronization across all systems. This 30-second threshold means that the new systems may not be adequately synchronized with the NTP server for up to 30 seconds, potentially resulting in inconsistent time stamps across systems. This is not compliant with the practice's requirement for uniform time stamps.

14.

When assessing an OSC?s compliance with IR requirements, you realize they have deployed a system that tracks incidents, documents details, and updates the status throughout the incident response process. Personnel to whom incidents must be reported are identified and designated. While examining their documentation, you come across an incident response template that they use to capture all relevant information and ensure consistency in reporting to the identified authorities and organizational officials. Interviewing the IR team, you learn there is an escalation process that the contractor?s cybersecurity team can use to address more serious incidents. From the scenario, the contractor has met all the required objectives for CMMC practice IR.L2-3.6.2-Incident Reporting, meaning its implementation of the said practice will be scored MET with a total of 5 points. For how long must the OSC retain the incident records?

90 days

72 days

72 hours

90 hours

Although CMMC doesn?t explicitly define the period by which the contractor should retain the incident-related records, DFARS 252.204-7012 is perhaps the best point of reference. Under the clause, the contractor should store such information for 90 days. This would allow the DoD to request information that can aid in their investigations, if necessary.

15.

During your assessment of Defcon's (a contractor) implementation of CMMC Level 2 practices, you notice that their system for displaying security and privacy notices is insufficient. The banners currently in use lack detailed information about Controlled Unclassified Information (CUI) handling requirements and associated legal implications. Additionally, the banners are not consistently displayed across all contractor systems and workstations. Moreover, the banners on login pages disappear automatically after less than 5 seconds, providing insufficient time for users to read and acknowledge the content. What is the biggest threat to the security of Defcon's systems from this scenario?

The biggest threat to the security of Defcon's systems is a lack of consistent user awareness and understanding of security and privacy responsibilities, particularly regarding Controlled Unclassified Information (CUI) handling.

The banners were too brief, providing insufficient time for users to read and acknowledge important security and privacy information.

The security and privacy banners were not integrated with mandatory user acknowledgment mechanisms, reducing their effectiveness in ensuring compliance.

The banners failed to include clear instructions or links to additional resources for proper CUI handling procedures, leaving users without guidance on next steps.

Inconsistent Display of Banners: If security and privacy notices, including those related to CUI handling, are not consistently displayed across all systems and workstations, some users may not be aware of their responsibilities or the importance of properly handling CUI. This inconsistency increases the risk of mishandling sensitive information. Insufficient Display Time: The fact that banners disappear after less than 5 seconds significantly reduces the likelihood that users will read, understand, and acknowledge the content. This can lead to users missing critical information about their legal obligations and the consequences of mishandling CUI. Lack of Specific Details: Banners that do not provide detailed information about CUI handling and legal implications fail to adequately inform users of the specific actions they need to take to protect sensitive information.

16.

You are assessing a contractor that develops missile guidance software containing CUI data. The software developers have administrative privileges on their workstations to be able to install tools and edit configuration files needed for their jobs. However, you have noted that many of the developers have access to modify components critical to system security, which is beyond what is needed for their specific roles. Which of the following is a potential risk if AC.L2-3.1.5, Least Privilege is not properly implemented for developers?

Unauthorized changes leading to vulnerabilities

Excessive workflow disruptions

Impacts to patch and update processes

Inability to complete projects timely

Providing excess privileges beyond what is needed for a specific role risks developers making unintended or malicious changes that could introduce vulnerabilities. This potential risk highlights the importance of adhering to least privilege.

17.

You are assessing a contractor that develops software for air traffic control systems. In reviewing their documentation, you find that a single engineer is responsible for designing new ATC system features, coding the software updates, testing the changes on the development network, and deploying the updates to the production ATC system for customer delivery. What would you recommend the contractor do to avert the risk?

Fully implement AC.L2-3.1.4, Separation of Duties by assigning different engineers responsibility for design, coding, testing, and deployment. Implement peer code reviews and separate test and deployment duties.

Increase the engineer's salary to incentivize careful work.

Institute mandatory overtime for the engineer to complete tasks faster.

Invest in more powerful development machines.

Implementing a Separation of Duties practice, directly addresses the identified risk. Separating the duties of design, code, test, deploy and implementing peer reviews creates a system where errors and malicious actions are more likely to be caught.

18.

During the Awareness and Training (AT) domain assessment, you examine the company's security awareness and training program. All new hires undergo a one-time security awareness training session during their onboarding process. After that, the IT department sends periodic email reminders about general security best practices, such as password management and phishing awareness. The contractor also offers an annual refresher training for managers and supervisors, covering topics related to data protection and incident response procedures. However, chatting with personnel from different roles, you discover personnel responsible for managing the company's networks and systems have yet to receive any specific training on secure configuration practices or identifying potential security risks associated with their roles. Production line workers and technicians handling CUI data during the manufacturing process are unaware of the specific security risks or procedures for handling and protecting CUI. Which of the following techniques can the contractor use to attain compliance with AT.L2-3.2.1-Role-Based Risk Awareness?

Develop and deliver role-specific training for personnel managing networks and systems, and provide specialized training to production line workers and technicians, covering secure configuration practices, identifying potential security risks associated with their roles, and handling CUI appropriately.

Install antivirus software on all user devices to prevent malware infections.

Implement advanced firewalls to protect against unauthorized access.

Regularly update and patch software to fix security vulnerabilities

---

Role-specific training ensures that the content is directly relevant to the tasks and responsibilities of each role. For example, network administrators need to understand secure configuration practices, while those handling Controlled Unclassified Information (CUI) must know how to protect that data. This targeted approach reduces the risk of security incidents by equipping personnel with the specific knowledge and skills they need to identify and mitigate the threats they are most likely to encounter in their daily work. Focus on High-Risk Areas: Personnel managing networks and systems typically have access to critical infrastructure and sensitive data. Training them on secure configuration and risk identification is crucial because mistakes in these areas can lead to significant security breaches, such as unauthorized access, data leaks, or system downtime. By focusing on high-risk areas relevant to each role, the training effectively reduces the likelihood of such breaches. The other options do not directly address the requirement: Installing antivirus software: This is a technical control rather than a training or awareness initiative, so it doesn't directly address the requirement for role-based risk awareness. Implementing

advanced firewalls: This is also a technical control, not related to security awareness or training. Regularly updating and patching software: This is a security practice rather than a training or awareness technique, so it does not fulfill the requirement for role-based training.

19.

When examining a contractor's access control policy and SSP, you observe that system administrators routinely use accounts with elevated privileges for checking email and browsing internal web sites. Why is it critical to implement practice AC.L2-3.1.6-Non-Privileged Account Use?

Reduces exposure to threats that might exploit the misuse of privileges

Mitigates the consequences of a security breach by safeguarding against data loss.

Enables easier auditing and logging of privileged activities.

Prevents unauthorized modification of security functions.

By requiring the use of non-privileged accounts for common non-security functions like email and web browsing, the exposure from potential compromise or misuse of privileged accounts is reduced.

20.

You are assessing Conedge Ltd, a contractor that develops cryptographic algorithms for classified government networks. In reviewing their network architecture documents, you see they have implemented role-based access controls on their workstations using Active Directory group policies. Software developers are assigned to the "Dev_Roles" group which grants access to compile and test code modules. The "Admin_Roles" group with elevated privileges for system administration activities is restricted to the IT staff. However, when you examine the event logs on a developer workstation, you find evidence that a developer was able to enable debugging permissions to access protected kernel memory - a privileged function. Which of the following implementation deficiencies allowed the developer to carry out a privileged function?

Improper role assignments.

Lack of account review procedures.

Insufficient network segmentation

Weak account credential requirements.

Improper role assignments enabled the developer to carry out privileged functions outside their responsibilities. The Dev_Roles group likely inherited permissions from Admin_Roles inappropriately. This type of privilege creep, where a non-privileged role inherits elevated permissions, enables users to execute actions well outside their responsibilities and job functions. The Dev_Roles group should have only the explicit privileges needed for software development and testing. Allowing it to inherit the elevated Admin_Roles permissions violates the principles of least privilege and separation of duties.

21.

When examining a contractor's security configuration settings, you find they have thoroughly documented the essential ports, protocols, services, and programs required for their business operations. They follow industry security configuration standards, such as CIS Benchmarks, to ensure systems are securely configured and hardened. Interviewing the network administrator and reviewing their processes, you learn that the contractor has implemented a rigorous whitelisting approach to control the execution of programs on their systems. Only applications and services that are deemed necessary for the system's function are explicitly allowed to run and are tightly controlled. They use Secure File Transfer Protocol (SFTP) services on port 22, Simple Mail Transfer Protocol (SMTP) on port 25, and DNS services on port 53, while restricting all other unnecessary ports and services using robust firewall configurations. The contractor conducts regular reviews of system services and functionalities to identify and disable any nonessential components that may have been inadvertently enabled or introduced through software updates or changes. They maintain a comprehensive inventory of all approved software, ports, protocols, and services, which is regularly audited and reconciled against the actual system configurations.Which other Configuration Management practice does CM.L2-3.4.7-Nonessential Functionality extend?

CM.L2-3.4.6 ? Least Functionality

CM.L2-3.4.3 ? System Change Management

CM.L2-3.4.1 ? System Baselining

CM.L2-3.4.5 ? Access Restrictions for Change

As stated in the CMMC Assessment Guide - Level 2, CMMC practice CM.L2-3.4.7-Nonessential Functionality, requires contractors to limit functionality to only essential programs, ports, protocols, and services, which extends the requirements of CMMC practice CM.L2-3.4.6-Least Functionality. CM.L2-3.4.6 requires adherence to the principle of least functionality but does not specifically address which elements of a system should be limited.

22.

During an interview with network administrators responsible for managing remote access, they mentioned using a next-generation firewall (NGFW) to secure the VPN connection, which can inspect remote device configurations and identify signs of potential split tunneling. How can the functionality of this NGFW contribute to achieving the objectives of CMMC practice SC.L2-3.13.7-Split Tunneling?

By detecting and potentially blocking remote device connections that exhibit signs of split tunneling.

By automatically reconfiguring remote devices to disable split tunneling.

By encrypting all traffic on the local network, the system can prevent unauthorized access even if split tunneling occurs.

By creating a centralized repository of allowed split-tunnel configurations for different user groups.

While automatically reconfiguring remote access devices might seem desirable, modifying them without proper authorization or central management could be disruptive. The NGFW?s ability to detect potential split tunneling attempts is valuable. By identifying such connections, the NGFW can take further actions, such as blocking them or alerting administrators for investigation. This proactive approach helps enforce CMMC practice SC.L2-3.13.7-Split Tunneling by mitigating the risks associated with split tunneling.

23.

An OSC can use either of the following strategies to meet the requirements of CMMC practice MP.L2-3.8.8-Shared Media, EXCEPT?

Permitting unrestricted use of portable storage devices after users complete security awareness training

Ensuring every portable storage device is assigned an owner, project, or department with an identifiable label or registered in a central database.

Implementing strong access controls that only allow registered devices to connect to the system.

Implementing a strict usage policy that allows for the use of owned portable or owned storage devices

---

The main assessment objective in CMMC practice MP.L2-3.8.8-Shared Media is ensuring that "the use of portable storage devices is prohibited when such devices have no identifiable owner." All the other options fulfil this objective. Permitting unrestricted use of portable storage devices is contrary to the requirements of the assessment objective, even if the users have completed a security awareness training program.

24.

You are conducting a CMMC assessment for a contractor that develops software applications for the DoD. During the assessment of the AU domain, you request to examine the contractor's audit and accountability policies, access control procedures, and system configuration documentation related to the management of audit logging functionality. Upon reviewing the documentation, the contractor has implemented an Role-Based Access Control (RBAC) model, where privileged users are assigned different roles based on their responsibilities. One of these roles is the "Audit Administrator" role, which is granted the necessary privileges to manage audit logging functionality across the contractor's systems. However, during interviews with the system administrators, you learn that besides the Audit Administrator role, several other privileged roles, such as the "System Administrator" and "Network Administrator" roles, can also manage audit logging functionality. When you inquire about the rationale behind granting multiple privileged roles access to audit management functions, the contractor's security team explains that this approach allows for better operational flexibility and ensures that different teams can perform audit logging tasks based on their areas of responsibility. Which assessment methods would be most appropriate for the assessor to evaluate the contractor's implementation of AU.L2-3.3.9-Audit Management?

A combination of examining relevant documentation, conducting interviews, and testing access management mechanisms.

Examine the system configuration settings and access control lists.

Interview personnel with audit and accountability responsibilities.

Test the mechanisms for managing access to audit logging functionality.

AU.L2-3.3.9-Audit Management suggests using a combination of assessment methods, including examining policies, procedures, system documentation, access authorizations, and system-generated lists of privileged users with access to audit management functions. Interviews with relevant personnel and testing the mechanisms for managing access to audit logging functionality are also recommended.

25.

Upon examining a contractor's Security and awareness training policy for compliance with AT.L2-3.2.2-Role-Based Training, you determine that they offer their employees training on handling CUI securely. However, system auditors, system administrators, penetration testers, and other cybersecurity roles are all provided biannual training on CUI handling and cybersecurity best practices. In your assessment, you would rely on all of the the following evidence, EXCEPT?

Codes of Federal Regulation

The contractor's training records

Security awareness and training policy

The contractor's security training curriculum and materials

While important for overall compliance, codes of federal regulations (CFRs) don't provide specific details about the contractor's implementation of role-based security training programs. CMMC focuses on the organization's internal practices and how they address the control requirements. However, you can examine the CFRs to determine what the contractor is required to comply with.

26.

You are conducting a CMMC assessment for a contractor that handles sensitive defense project data. Reviewing their documentation shows that the Contractor has an on-premises data center that houses CUI on internal servers and file shares. A corporate firewall protects this data center network. However, the Contractor also uses a hybrid cloud infrastructure, storing some CUI in Microsoft Azure cloud storage, which can be accessed using ExpressRoute private network connections. Additionally, their engineers connect remotely to the data center to access CUI via a site-to-site VPN from their home networks. What risks does the hybrid infrastructure with cloud storage and remote access introduce regarding CUI data flow?

It increases the number of entry and exit points for CUI data. The remote access also makes auditing and controlling flow more difficult.

Increases chances of CMMC non-compliance

Exposes the data to unauthorized access.

It has no impact on CUI data flow or risks.

By introducing cloud storage and remote access, there are more entry points for potential breaches. This wider access also makes it harder to track and control CUI data movement, increasing the risk of unauthorized access and making it more difficult to ensure compliance with data security regulations.

27.

Unique individuals, processes, and devices must be assigned Identifiers. CMMC requires that an OSC defines a period of inactivity after which an identifier is disabled. The identifier must be disabled after the defined period of inactivity lapses. All of the following are effective strategies the OSC can use to meet the requirements of CMMC practice IA.L2-3.5.6-Identifier Handling, EXCEPT?

Subscribing to RSS feeds

Automated monitoring and periodic auditing and administrator review

Setting up automated alerts and implementing a secure reactivation process

Implementing an automated inactivity threshold policy

To fulfil CMMC practice IA.L2-3.5.6-Identifier Handling, the OSC can adopt a blend of strategies for managing account inactivity. Implementing automated monitoring to track and turn off unused identifiers after a specified inactivity period, alongside generating activity reports to flag such accounts, effectively manages inactivity. An inactivity threshold policy, supported by administrator reviews and account management tools, ensures automated deactivation of inactive accounts. Automated alerts can inform administrators about accounts nearing inactivity thresholds, complemented by periodic system usage audits. Training on the importance of deactivating unused accounts, a clear usage policy on inactivity thresholds, and a secure process for account reactivation collectively enhance security by minimizing risks associated with inactive accounts, aligning with CMMC requirements.

28.

While reviewing a contractor's Microsoft Active Directory authentication policies, you observe that the account lockout threshold is configured to allow 5 consecutive invalid login attempts before locking the account for 15 minutes. Additionally, the reset account lockout counter is set to 30 seconds after each unsuccessful login attempt. Based on this scenario, which of the following statements are TRUE about the contractor's implementation of CMMC practice AC.L2-3.1.8-Unsuccessful Logon Attempts?

The contractor has successfully implemented practice AC.L2-3.1.8-Unsuccessful Logon Attempts warranting a score of MET

Based on the current implementation, CMMC practice AC.L2-3.1.8 cannot be scored as MET.

The contractor's approach does not provide sufficient protection against unauthorized access attempts.

The contractor's approach does not adequately address the required assessment objectives

---

Although there may be other better ways of implementing means of limiting unsuccessful logon attempts, the contractor has demonstrated to have taken sufficient measures to meet the two assessment objectives of AC.L2-3.1.8 including setting the account lockout threshold, reset account lockout counter, and account lockout duration.

29.

An OSC has documented HR and personnel security policies, which are well integrated. A key requirement is that credentials and systems are revoked upon a transfer or termination. Their personnel security policy includes procedures for transfer and termination, a list of system accounts tied to each employee, and management of revoked or terminated credentials and authenticators. Examining the procedures addressing personnel transfer and termination, you learn that besides revoking or terminating system access, authenticators, and credentials, the OSC recovers all company IT equipment, access/identification cards, and keys from the transferred or terminated employee. They also interview the employee to remind them of their CUI handling obligations even after transfer and require them to sign an NDA. After every termination, they also change the password and other access control mechanisms and notify all the stakeholders that the employee has been terminated or transferred. Based on the scenario, the OSC can cite the following as evidence of collaborating on their implementation of CMMC practice PS.L2-3.9.2-Personnel Actions, EXCEPT?

List of usernames and passwords of all the employees

Records of personnel transfer and termination actions

Records of exit interviews accompanied by a list of terminated employees' identifiers

Records of terminated or revoked authenticators and credentials

---

Although a security best practice, CMMC practice PS.L2-3.9.2-Personnel Actions, does not require maintaining a list of usernames and passwords for all employees. The other evidence (personnel transfer/termination actions, revoked authenticators/credentials, exit interviews with terminated employees' identifiers) are relevant for demonstrating compliance with this practice.

30.

You are assessing a contractor that develops software for air traffic control systems. In reviewing their documentation, you find that a single engineer is responsible for designing new ATC system features, coding the software updates, testing the changes on the development network, and deploying the updates to the production ATC system for customer delivery. What risks does this pose related to separation of duties?

The engineer has too much concentrated privilege which increases risk of errors or malicious activity.

The development timeline might be delayed.

The engineer might forget important details during the development process.

The engineer's role and responsibilities in the development process are clearly defined.

Having a single engineer handle all stages increases the risk of errors going unnoticed. Malicious actors could also exploit this situation to introduce vulnerabilities undetected. (AC.L2-3.1.4, Separation of Duties) requires the separation of duties to create checks and balances, mitigate such risks.

31.

A defense contractor has implemented a secure wireless network infrastructure to support their operations and client engagements. They use the WPA2-Enterprise encryption protocol with AES-CCMP ciphers and the 802.1X port-based authentication framework to secure their wireless network. The wireless network infrastructure includes a Remote Authentication Dial-In User Service (RADIUS) server for centralized authentication and authorization of wireless clients. The contractor has deployed multiple Wireless Access Points (WAPs) throughout their office premises, each with its own Service Set Identifier (SSID) and VLAN configuration. Before granting wireless access, the contractor?s IT team verifies the device's compliance with their security standards and validates the user's credentials against the RADIUS server using EAP-TLS authentication. Based on the scenario, which of the following recommendations would be MOST appropriate for the contractor to improve their security posture under AC.L2-3.1.16-Wireless Access Authorization?

Implementing additional network segmentation to isolate sensitive data from other network traffic.

Replacing the 802.1X framework with a simpler password-based authentication mechanism.

Disabling individual SSID and VLAN configurations on each WAP for a more centralized approach.

Increasing the frequency of wireless password changes for all users accessing the network.

Based on the scenario, the MOST appropriate recommendation for the contractor to improve their security posture under AC.L2-3.1.16 - Wireless Access Authorization is: Implementing additional network segmentation to isolate sensitive data from other network traffic. Network Segmentation: Enhancing network segmentation further isolates sensitive data, reducing the risk of unauthorized access and limiting the impact of any potential breach. This directly supports the protection of Controlled Unclassified Information (CUI) and aligns with best practices for secure wireless access authorization. Other options, 1) replacing 802.1X with password-based authentication would weaken security, as 802.1X provides stronger, more secure authentication methods compared to simpler password-based mechanisms; 2) disabling individual SSID and VLAN configurations would reduce the granularity of control and segmentation, potentially lowering security rather than improving it; and 3) increasing the frequency of wireless password changes might improve security to a degree, but it is not as impactful or aligned with the specific requirements of wireless access authorization under CMMC as implementing additional segmentation.

Therefore, implementing additional network segmentation is the most appropriate recommendation for improving the contractor's security posture.

32.

Examining an OSC password policy, you learn that a password should have a minimum of 15 characters. It also should have 3 uppercase, 2 special characters, and other alphanumeric characters. Passwords have to be changed every 45 days and cannot be easily tied to the account owner. Passwords cannot be reused until 30 cycles are complete. The OSC's systems send a temporary password to the user's email or authentication app, which is one of the events described in their password usage policy. However, a recent penetration test report shows that the generated temporary passwords did not have sufficient entropy, and an attacker may guess a temporary password through brute force attacks. How would you score the contractor's implementation of the IA domain requirement on Temporary Passwords?

Not Met (-1 point)

Met (+5 points)

Met (+1 point)

Not Met (-5 points)

The penetration test report shows that the generated temporary passwords did not have sufficient entropy, making them vulnerable to brute-force attacks. This does not align with the requirement in CMMC practice IA.L2-3.5.9-Temporary Passwords, which requires passwords to be changed immediately to a permanent password upon logon, ensuring the necessary strength of the authentication mechanism. While the contractor has a temporary password usage policy, the implementation fails to provide secure temporary passwords that must be changed right away, as required by ICMMC practice IA.L2-3.5.9-Temporary Passwords.

33.

A medium-sized company that develops software components for DoD's military applications has a dedicated IT team responsible for maintaining its infrastructure and systems. They have retained your services to assess their compliance with CMMC requirements for certification so they can continue offering services to the DoD. Recently, the contractor experienced several security incidents where unauthorized changes were made to their systems, resulting in potential data breaches and system instability. Upon investigation, it was discovered that some IT team members were using unauthorized tools and techniques for system maintenance, and there was a lack of proper controls and oversight over the maintenance processes. Which measures should the contractor implement to comply with CMMC practice MA.L2-3.7.2-System Maintenance Control?

Establish and enforce policies and procedures for approving, controlling, and monitoring maintenance tools, techniques, and mechanisms.

Outsource all system maintenance activities to a third-party vendor to avoid potential issues.

Provide unrestricted access to maintenance tools and techniques for all IT personnel to facilitate efficient maintenance activities.

Implement strict access controls for maintenance personnel but allow them to use any necessary tools and techniques.

CMMC practice MA.L2-3.7.2-System Maintenance Control requires organizations to provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. Establishing and enforcing policies and procedures that govern the approval, control, and monitoring of maintenance tools, techniques, and mechanisms directly addresses this requirement.

34.

During your assessment of an OSC's implementation of security engineering principles throughout its system and software development lifecycles, you review their policies and interview personnel. The OSC has a documented security architecture that includes high-level security requirements such as data encryption, least privilege access controls, and input validation. However, this guidance remains fairly general. You then examine the system design documentation for a key application processing CUI. Although security requirements are mentioned, there is no evidence that specific security engineering techniques?such as threat modeling, layered protections, or secure design patterns?were employed during the design phase. Interviews with the development team reveal limited experience with advanced security engineering practices beyond basic secure coding. The team admits they did not perform activities like misuse case analysis, abuse case modeling, or attack surface reviews during the design process. In further testing, you find that the OSC has established secure coding standards, conducts static code analysis, and performs penetration testing before production releases. However, there are no documented processes for incorporating explicit security engineering activities during the design and architecture phases. Based on this scenario how does the lack of documented processes for security engineering activities during the design and architecture phases most likely impact the security of the OSC?s CUI? Chose the best answer

Security vulnerabilities are likely to be introduced during the design phase and may remain undetected throughout the development lifecycle.

Secure coding practices and penetration testing will still identify most vulnerabilities.

It makes it more difficult for developers to understand the security requirements.

The OSC will not be able to comply with other CMMC security practices.

The lack of documented security engineering activities during the design and architecture phases increases the risk of vulnerabilities being embedded in the system's foundation, which may not be identified or mitigated later in the development lifecycle, even with secure coding practices and testing, potentially exposing CUI to threats.

35.

An engineering company works on DoD contracts that involve handling CUI. They use hardcopy media such as printed paper, microfilms, and digital media, including flash drives, SSDs, DVDs, and internal and external hard drives. During a CMMC assessment, you discover the engineering company has defined procedures addressing media storage and access governed by an access control policy. All media containing CUI is marked and stored in biometrically locked cabinets. To store CUI on digital media, an authorized user must be identified using their biometrics or authenticated using an integrated MFA solution. To access non-digital media, the user must be on a defined list of authorized personnel and sign three forms. You also learn that the contractor maintains a comprehensive inventory of all CUI media. Basing your answer on the scenario, how would you score the contractor?s implementation of CMMC practice MP.L2-3.8.1-Media Protection?

Met

Not Met

Not Applicable

Partially Met

The contractor meets the CMMC practice MP.L2-3.8.1-Media Protection requirements showing strengths in inventory management, access control, and secure storage of Controlled Unclassified Information (CUI) media, with biometric cabinets and Multi-Factor Authentication (MFA) for digital access.

36.

You are conducting a CMMC assessment for a contractor that develops software applications for the DoD. During the assessment of the AU domain, you request to examine the contractor's audit and accountability policies, access control procedures, and system configuration documentation related to the management of audit logging functionality. Upon reviewing the documentation, the contractor has implemented an Role-Based Access Control (RBAC) model, where privileged users are assigned different roles based on their responsibilities. One of these roles is the "Audit Administrator" role, which is granted the necessary privileges to manage audit logging functionality across the contractor's systems. However, during interviews with the system administrators, you learn that besides the Audit Administrator role, several other privileged roles, such as the "System Administrator" and "Network Administrator" roles, can also manage audit logging functionality. When you inquire about the rationale behind granting multiple privileged roles access to audit management functions, the contractor's security team explains that this approach allows for better operational flexibility and ensures that different teams can perform audit logging tasks based on their areas of responsibility. Based on the information provided in the scenario, how would you assess the contractor's compliance with CMMC practice AU.L2-3.3.9-Audit Management?

Not Met - The contractor has granted audit management privileges to multiple privileged roles, which goes against the requirement to limit access to a subset of defined privileged users.

Met - The contractor has defined privileged user roles for audit management.

Partially Met - The contractor has limited audit management privileges to a subset of privileged users, but the roles may not be appropriately defined.

Not Applicable - The practice is not relevant to the contractor's environment.

According to the scenario, the contractor has granted the ability to manage audit logging functionality to several privileged roles, such as System Administrators and Network Administrators, in addition to the Audit Administrator role. This goes against the requirements of CMMC practice AU.L2-3.3.9-Audit Management, to limit the management of audit logging functionality to a defined subset of privileged users.

37.

Organizations have to control what systems can be installed for the principle of least functionality to apply. You assess the contractor's implementation of Configuration Management requirements and start by examining their documentation. They maintain a regularly updated inventory of authorized software to support their allowlisting and blocklisting efforts. The contractor has configured their information systems such that only authorized software can be executed or installed after software approval. Any attempts to install unauthorized software by unauthorized personnel are automatically logged, and an alert is sent to the system administrator. To meet the requirements of CM.L2-3.4.8-Application Execution Policy the contractor can use the strategies below, EXCEPT?

Encrypting data at rest and in transit

Ensuring all software installed on their systems have undergone a rigorous approval process

Ensuring the use of automated configuration management tools

Application blocklisting and allowlisting

The contractors have leveraged various strategies to address the requirements of practice CM.L2-3.4.8-Application Execution Policy, including maintaining and regularly reviewing an inventory of allowed and prohibited applications. They are leveraging a software approval process to vet and authorize software before installation into organizational systems. Additionally, they use an automated tool that monitors unauthorized attempts to install software, logs violations and sends alerts to the system administrator.

38.

While examining a contractor's audit and accountability policy, you realize they have documented types of events to be logged and defined content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. After the logs are analyzed, the results are fed into a system that automatically generates audit records stored for 30 days. However, mechanisms implementing system audit logging are lacking after several tests because they produce audit logs that are too limited. You find that generated logs cannot be independently used to identify the event they resulted from because the defined content specified therein is too limited. Additionally, you realize the logs are retained for 24 hours before they are automatically deleted. Which of the following is a potential assessment method for AU.L2-3.3.1-System Auditing?

Examine procedures addressing audit record generation

Testing the system configuration settings and associated documentation

Examining the mechanisms for implementing system audit logging

Testing procedures addressing control of audit records

System configuration settings and procedures addressing control of audit records need to be examined while mechanisms are implemented. Thus, the only potential assessment method consistent with the definition provided in NIST SP 800-171A and CMMC practice AU.L2-3.3.1 is examining audit record generation procedures.

39.

Examining an OSC?s system design documentation, you notice they have implemented a CUI enclave and have a documented procedure addressing boundary protection. They have segmented their network into different zones, each having its own rules to allow or deny traffic. The OSC has implemented strict firewall rules that deny all incoming and outgoing traffic by default, only allowing specific traffic as required. To automatically block unrecognized traffic patterns, the OSC has provisioned a state-of-the-art Intrusion Detection and Prevention System (IDPS). During an interview with the network administrator, you realize that OSC uses a whitelisting approach to explicitly allow only certain IP addresses, domains, or services to communicate with their system. Their IT security team monitors network traffic to detect any unauthorized attempts to connect or communicate with their system. The scenario states that network traffic is monitored to detect unauthorized connection attempts. Which of the following best describes the purpose of monitoring network traffic in the context of CMMC practice SC.L2-3.13.6-Network Communication by Exception?

To identify and potentially respond to suspicious or anomalous traffic patterns that might indicate attempted breaches.

To identify and automatically add to the allowlist new legitimate communication requests.

To verify that firewall rules are correctly configured and functioning as intended.

To generate reports on network bandwidth usage for capacity planning purposes.

CMMC practice SC.L2-3.13.6-Network Communication by Exception requires organizations to deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). Monitoring network traffic in this context serves to identify and potentially respond to suspicious activity that might violate the deny-all principle of SC.L2-3.13.6. This proactive approach helps detect potential breaches and mitigate risks.

40.

CMMC practice CM.L2-3.4.9-User-Installed Software, requires OSCs to establish a policy controlling software installation, ensure any software installations by any user follow the established policy, and monitor user software installation. Which of the following is not something the OSC can cite as evidence to demonstrate their efforts to meet the requirements of CM.L2-3.4.9-User-Installed Software?

Installed software specifications

The OSC's formal process for users to request the installation of approved software

The OSC's procedures addressing user-installed software

The list of rules governing user-installed software

An OSC can demonstrate meeting the requirements of CMMC practice CM.L2-3.4.9-User-Installed Software, for controlling and monitoring user-installed software through: 1) A list of rules governing user software installations, addressing the need for an established policy [a]. 2) Documented procedures on user-installed software, showing how the policy is implemented [b]. 3) A formal process for users to request approved software installations, enabling monitoring of installations [c]. These processes comprehensively cover having a software installation policy, enforcing it through procedures, and a mechanism to track approved user installations, fully satisfying the practice objectives. Installed software specifications cannot be used as evidence in this scenario as it is unknown who installed the software and if the process to request and intall software was followed.

41.

When assessing a contractor?s implementation of CMMC practices, you examine its System Security Plan (SSP) to identify its documented measures for audit reduction and reporting. They have a dedicated section in their SSP addressing the Audit and Accountability requirements. You proceed to interview their information security personnel, who informed you that the contractor has a dedicated Security Operations Center (SOC) and uses Splunk to reduce and report audit logs. What key features regarding the deployment of Splunk for AU.L2-3.3.6-Reduction & Reporting, would you be interested in assessing?

Ensure that Splunk employs various filter rules for reducing audit logs to eliminate non-essential data and processes to analyze large volumes of log files or audit information, identifying anomalies and summarizing the data in a format more meaningful to analysts. Thus generating customized reports.

Ensue Splunk can retain audit records for a protracted amount of time

Ensure Splunk can support compliance dashboards that provide real-time visibility into CMMC compliance status

Ensure that Splunk is configured with appropriate RBAC to restrict access to log data, reports, and dashboards, ensuring that only authorized personnel can view or modify audit logs.

To assess compliance with AU.L2-3.3.6-Reduction & Reporting, you would want to understand how Splunk collects logs from relevant sources, processes and reduces the audit logs [a], and generates reports from the audit data [b]. The practice requires the organization to provide audit reduction and report generation capabilities.

42.

During your assessment of an OSC's implementation of security engineering principles throughout its system and software development lifecycles, you review their policies and interview personnel. The OSC has a documented security architecture that includes high-level security requirements such as data encryption, least privilege access controls, and input validation. However, this guidance remains fairly general. You then examine the system design documentation for a key application processing CUI. Although security requirements are mentioned, there is no evidence that specific security engineering techniques?such as threat modeling, layered protections, or secure design patterns?were employed during the design phase. Interviews with the development team reveal limited experience with advanced security engineering practices beyond basic secure coding. The team admits they did not perform activities like misuse case analysis, abuse case modeling, or attack surface reviews during the design process. In further testing, you find that the OSC has established secure coding standards, conducts static code analysis, and performs penetration testing before production releases. However, there are no documented processes for incorporating explicit security engineering activities during the design and architecture phases. For an OSC?s legacy applications, what does CMMC practice SC.L2-3.13.2-Security Engineering require regarding the application of security engineering principles?

Principles should be applied to the extent feasible based on the current state of the component.

You must retroactively apply security engineering principles to all legacy components.

You must re-architect and remediate all legacy components to align with the security engineering principles.

There is no requirement to apply security engineering principles to legacy components, only to new development.

CMMC practice SC.L2-3.13.2-Security Engineering states that for legacy systems, organizations should apply security engineering principles ?to the extent feasible, given the current state of hardware, software, and firmware components within those systems.? Therefore, retroactively applying principles is expected where possible, without necessarily requiring a full re-architecture.

43.

A medium-sized company that develops software components for DoD's military applications has a dedicated IT team responsible for maintaining its infrastructure and systems. They have retained your services to assess their compliance with CMMC requirements for certification so they can continue offering services to the DoD. Recently, the contractor experienced several security incidents where unauthorized changes were made to their systems, resulting in potential data breaches and system instability. Upon investigation, it was discovered that some IT team members were using unauthorized tools and techniques for system maintenance, and there was a lack of proper controls and oversight over the maintenance processes. According to CMMC practice MA.L2-3.7.2-System Maintenance Control, which of the following controls should the contractor implement for personnel involved in system maintenance?

Implement strict access controls and monitoring mechanisms for maintenance personnel.

Rely on maintenance personnel's professional certifications as sufficient vetting.

Only allow maintenance personnel to work during off-hours to minimize operational disruptions.

Maintenance personnel should be provided unrestricted access to all systems and components.

CMMC practice MA.L2-3.7.2-System Maintenance Control states that organizations should control the "personnel used to conduct system maintenance." Implementing access controls and monitoring mechanisms for maintenance personnel fulfils this requirement. Strict controls and agreements with external maintenance service providers are also critical to ensure they adhere to organizational standards and do not introduce new issues.

44.

In assessing an OSC's CUI handling practices, you learn they use an approved algorithm (AES-256) to encrypt the data to ensure its confidentiality. However, the encryption module they are using has not been validated under the FIPS 140 standard. The OSC believes that using an approved algorithm is sufficient to comply with the CMMC practice for CUI encryption requirements. Based on the information provided, is the OSC compliant with CMMC practice SC.L2-3.13.11-CUI Encryption? How would you score their implementation of this practice?

No, the OSC is not compliance. This practice would be scored as a deduction of 3 (-3) points.

Yes, 5 points.

Partially compliant; 1 point.

More information is needed to determine compliance.

The practice CMMC practice SC.L2-3.13.11-CUI Encryption explicitly requires the use of FIPS-validated cryptography to protect the confidentiality of CUI. Using an approved algorithm alone is not sufficient; the cryptographic module (software or hardware) must be validated under the FIPS 140-2 or FIPS 140-3 standard. According to the DoD scoring methodology for this practice, if no cryptography is applied to protect CUI confidentiality, the assessor subtracts 5 points. However, if the OSC has applied cryptography to secure CUI but the modules are not FIPS 140-2 or 140-3 validated, the assessor subtracts 3 points.

45.

After a security audit, a contractor documents specific vulnerabilities and deficiencies in an audit report. After examining its POA&M, you realize it has a clearly defined policy on addressing these deficiencies and by when. However, after interviewing the contractor?s security and compliance team, you learn that while an audit is regularly conducted, the remediating measures are not always taken, and when taken, they are not always practical. The security and compliance team informs you they have tried reaching the system administrator to explain the repercussions of this without success. What assessment objective has the contractor failed to implement from CMMC practice CA.L2.3.12.2-Plan of Action?

Implement a plan of action to correct the identified deficiencies and reduce or eliminate identified vulnerabilities that are ineffective.

Identify the vulnerabilities and deficiencies that the plan of action will address.

Develop a change management plan that describes how to implement the remediation actions

The contractor has implemented all the assessment objectives in CA.L2-3.12.2-Plan of Action.

While the contractor has a defined remediation policy/plan and conducts regular audits to identify issues, the key failure point is that the remediation actions in the plan are not consistently taken or are ineffective when applied, according to interviews with the security and compliance team.

46.

After you ask to examine some audit records, the contractor's system admininstrator informs you that there is a process to follow before accessing them. The logs are hashed using SHA-512 algorithms, and the system administrator has to run an algorithm to recalculate the hashes for the audit records to verify their integrity before running a decryption algorithm to decrypt the data. Since this might take some time, you tour the facility while interviewing personnel with audit and accountability roles. You see an employee holding the door for another without using their physical access card. While interviewing the contractor's employees, you find that they can access all audit logging tools and tweak the settings according to their needs or requirements. Upon examining the contractor's access control policy, you realize they have not defined the measures to protect audit logging tools. How can the contractor improve their access control for audit logging tools?

Implement role-based access control (RBAC) to restrict access based on job duties.

Train employees on the importance of protecting audit logs and the consequences of unauthorized access.

Increase the complexity of algorithms used for hashing and encryption of audit records.

While access control is essential, focusing on employee awareness is sufficient for CMMC compliance.

Implementing Role-Based Access Control (RBAC) directly addresses the control requirement and ensures only authorized personnel have access to audit logging tools, whose access level is based on job responsibilities. While the other options have merit, they do not directly address access control.

47.

A defense contractor has implemented a secure wireless network infrastructure to support their operations and client engagements. They use the WPA2-Enterprise encryption protocol with AES-CCMP ciphers and the 802.1X port-based authentication framework to secure their wireless network. The wireless network infrastructure includes a Remote Authentication Dial-In User Service (RADIUS) server for centralized authentication and authorization of wireless clients. The contractor has deployed multiple Wireless Access Points (WAPs) throughout their office premises, each with its own Service Set Identifier (SSID) and VLAN configuration. Before granting wireless access, the contractor?s IT team verifies the device's compliance with their security standards and validates the user's credentials against the RADIUS server using EAP-TLS authentication. Based on the scenario, which of the following statements BEST describes the contractor's compliance with CMMC AC.L2-3.1.16-Wireless Access Authorization?

The scenario does not provide enough information to determine compliance with CMMC AC.L2-3.1.16-Wireless Access Authorization.

The contractor partially complies as they lack pre-approval for specific devices.

The contractor complies because they utilize strong encryption and authentication protocols.

The contractor does not comply because they use multiple WAPs with different configurations.

Based on the scenario provided, the contractor's compliance with CMMC AC.L2-3.1.16-Wireless Access Authorization can be inferred. Even though wireless access is authorized prior to allowing connections, it does not explicitly confirm that the Wireless Access Points (WAPs) themselves are uniquely identified as part of the authorization process. Wireless Access Authorization: The scenario states that the contractor?s IT team verifies device compliance with security standards and validates user credentials against the RADIUS server using EAP-TLS authentication before granting wireless access. This indicates that wireless access is authorized prior to connection. WAP Identification: While the scenario mentions that multiple WAPs are deployed with unique SSIDs and VLAN configurations, it does not explicitly state that the WAPs are identified or authorized as part of the connection process. However, the use of unique SSIDs and VLAN configurations implies a level of network segmentation and control. You can conclude that wireless access is authorized prior to allowing connections based on user and device authentication. However, the scenario does not explicitly confirm whether each WAP is uniquely identified as part

of the authorization process. If WAP identification and authorization are required for full compliance, this detail would need to be explicitly verified or included.

48.

You have been sent to assess an OSC?s implementation of CMMC practices, one of which is AC.L2-3.1.11-Ssession Termination. In assessing the contractor's implementation of AC.L2-3.1.11, you?ll likely need to examine the following specifications, EXCEPT?

Mechanisms for implementing user session termination

System Security plan

The Session termination policy

The Access control policy

Except for mechanisms for implementing user session termination, all the other items fit the definition of a specification provided in NIST SP 800-171A as ?documented artifacts? associated with a system. Plans, policies, procedures, requirements, functional and assurance specifications, architectures, and design documentation are some of specifications.

49.

When examining a contractor's access control policy and SSP, you observe that system administrators routinely use accounts with elevated privileges for checking email and browsing internal web sites. What CMMC practice does this violate?

AC.L2-3.1.6

AC.L2-3.1.7

AC.L2-3.1.4

AC.L2-3.1.2

The practice violates AC.L2.3.1.6, Non-privileged Account Use which requires the contractor to define non-security functions and require personnel to use non-privileged accounts or roles when accessing nonsecurity functions.

50.

Mobile devices are increasingly becoming important in many contractors? day-to-day activities. Thus, the contractors must institute measures to ensure they are correctly identified and any connections are authorized, monitored, and logged, especially if the devices or their connections process, store, or transmit CUI. You have been hired to assess a contractor?s implementation of CMMC practices, one of which is AC. L2.3.1.18 (Mobile Device Connections). To successfully test the access control capabilities authorizing mobile device connections to organizational systems, you must first identify what a mobile device is. Which of the following is not considered a mobile device?

Laptops

Tablets

E-Readers

Smartphones

The scope defined in NIST SP 800-124 Rev.2 states that laptops are specifically excluded from the scope of this publication as the security controls available today for laptops are quite different than those available for mobile phones, tablets, and other mobile device types. Mobile devices with minimal computing capability are excluded, including feature phones, wearables, and other devices included under the Internet of Things (IoT) umbrella

51.

Mobile devices are increasingly becoming important in many contractors? day-to-day activities. Thus, the contractors must institute measures to ensure they are correctly identified and any connections are authorized, monitored, and logged, especially if the devices or their connections process, store, or transmit CUI. You have been hired to assess a contractor?s implementation of CMMC practices, one of which is AC. L2.3.1.18 (Mobile Device Connections). To successfully test the access control capabilities authorizing mobile device connections to organizational systems, you must first identify what a mobile device is. Mobile devices connecting to organizational systems must have a device-specific identifier. Which of the following is the main consideration for a contractor when choosing an identifier?

Choosing an identifier that can accommodate all devices and be used consistently within the organization.

Use random identifiers to identify mobile devices on the network easily.

The identifier must be easily differentiable from one device to another.

Prioritize using identifiers that are easy to remember and user-friendly.

When choosing a device-specific identifier for mobile devices connecting to organizational systems, the primary consideration should be selecting an identifier that can be used consistently across all devices within the organization. This consistency is essential for properly identifying, tracking, and managing mobile devices on the network. The CMMC Assessment Guide emphasizes the importance of using a consistent and unique identifier for mobile devices to ensure proper access control, monitoring, and accountability within the organization?s systems.

52.

You are on-site with an Assessment Team at a medium-sized organization. When discussing how they protect their company's information from malware, spyware, etc., the administrator you are interviewing offers to show you the entire process from start to finish since she had that on her to-do list for the day. She opens the machine, turns it on, and installs what she says is anti-malware software. She also demonstrates how their deployed Next Generation Firewall (NGFW) works. You have never heard of this software, so you ask her where it was purchased. You later learn it is an open-source solution. Based on the scenario and the requirements of CMMC practice SI.L2-3.14.6-Monitor Communications for Attacks, what is your likely determination?

Request for more information.

Find the OSC's implementation of the practice as Met.

Fail the OSC's implementation of the practice.

Find the OSC's implementation as partially Met as they are achieving several objectives required of this practice.

Based on the scenario and the requirements of CMMC practice SI.L2-3.14.6, which focuses on monitoring communications for attacks, the use of open-source software is concerning due to the potentially untrusted nature of such software. Thus, requesting for more information and investigating further should provide the assessor with more details to make an informed decision. Unvetted Open-Source Software: The administrator is using an open-source anti-malware solution that you were not previously familiar with. While open-source solutions can be effective, their use introduces certain risks if they are not properly vetted, maintained, and updated. CMMC compliance requires ensuring that any tools used for monitoring and protecting information systems are reliable and effective. If the organization has not thoroughly vetted the open-source software, especially for potential vulnerabilities or if it lacks a process for keeping it up-to-date, this could be a concern. Furthermore, the use of an open-source solution for critical security functions like anti-malware protection, creates a potential compliance gap, as it might raise questions about whether the organization has adequately ensured that the software meets the necessary security standards. If the software is not recognized, validated, or frequently updated, it might not provide adequate protection against sophisticated attacks, potentially putting the organization at risk. The demonstration of the Next Generation Firewall (NGFW) is a positive step as NGFWs typically offer advanced features like deep packet inspection, intrusion prevention, and application awareness. However, for CMMC compliance, it?s crucial that the firewall is correctly configured, regularly monitored, and integrated into a broader security strategy that includes other defensive measures. It addresses objectives [b] and [c] by monitoring inbound

and outbound traffic to detect attacks and indicators of potential attacks. Part of CMMC compliance is having documented procedures and evidence of consistent monitoring and protective measures. You would need to ensure that the organization has documented the implementation and regular monitoring of their anti-malware and firewall solutions, including any specific processes for managing open-source software.

53.

When interviewing a contractor?s CISO, they inform you that they have documented procedures addressing security assessment planning in their security assessment and authorization policy. The policy indicates that the contractor undergoes regular security audits and penetration testing to assess the posture of its security controls every ten months. The policy also states that after every four months, the contractor tests its incident response plan and regularly updates its monitoring tools. Impressed by the contractor?s policy implementation, you decide to chat with various personnel involved in security functionalities. You realize that although it is documented in the policy, the contractor has not audited their security systems in over two years. Which of the following actions would best address the identified gap in the contractor?s implementation of CA.L2.3.12.1-Security Control Assessment?

Developing a plan to conduct security audits following the documented frequency in the policy and ensuring continuous adherence.

Updating the security policy to reflect the actual frequency of security audits

Assigning additional personnel to the security team to manage frequent assessments

Conducting immediate security audits without prior planning.

Developing and implementing a plan to conduct security audits resolves the core issue of not adhering to the stated assessment frequency policy. Developing a plan lays out the roadmap to get assessments back on track per the existing requirements rather than changing the policy. Ensuring this is followed going forward closes the gap.

54.

You are assessing Conedge Ltd, a contractor that develops cryptographic algorithms for classified government networks. In reviewing their network architecture documents, you see they have implemented role-based access controls on their workstations using Active Directory group policies. Software developers are assigned to the "Dev_Roles" group which grants access to compile and test code modules. The "Admin_Roles" group with elevated privileges for system administration activities is restricted to the IT staff. However, when you examine the event logs on a developer workstation, you find evidence that a developer was able to enable debugging permissions to access protected kernel memory - a privileged function. Which of the following controls could have prevented the developer from executing this privileged function?

Prohibiting inheritance of privileged permissions.

Enforcing dual authorization

Implementing time of day restrictions.

Removing internet access.

Explicitly defining the permissions for the Dev_Roles group, without allowing inheritance from Admin_Roles, would help enforce least privilege and separation of duties. The developers would retain only the specific privileges needed for their coding and testing work, without inheriting any elevated admin capabilities. Setting explicit privileges for each role, rather than relying on group nesting or inheritance, is a best practice for access control and aligns with the principles of least privilege and separation of duties in CMMC. This strict role definition prevents privilege creep and enforces segregation of duties across different teams and job functions.

55.

An OSC has an established Incident Response plan and a dedicated team specifically trained to handle any potential incidents and conduct necessary analysis. When performing the assessments, you also realize the OSC has deployed IDS and SIEM tools to identify possible incidents. Examining the Contractor's incident response policy, you also learn they have defined and implemented containment strategies and have developed clear procedures for system and data recovery after an incident, including backup and restore procedures. There is also a communication protocol in place to inform the affected stakeholders and users after a security incident. Chatting with a few members of the OSC's incident response team, you learn they conduct regular drills to test and improve the effectiveness of the incident-handling capability. There also are defined and documented incident response mechanisms and a post incident analysis procedure to identify lessons learned and make necessary improvements to the incident-handling process. Based on the information provided, the following aspects of IR.L2-3.6.1-Incident Handling can be definitively confirmed for the OSC's incident response capability, EXCEPT?

Risk tolerance

Preparation

Detection

Analysis

The OSC has established an incident response plan, a trained team, and user training, which indicates preparation. The use of IDS/SIEM tools suggests a focus on detection. There's no mention of specific analysis techniques, but a trained team implies some level of analysis capability. Additionally, there is no mention of the OSC's risk tolerance, which refers to the level of risk the organization is willing to accept before taking action or implementing additional controls. This aspect is crucial in defining how aggressively the OSC responds to different incidents but isn't covered in the provided details.

56.

You are assessing a contractor with a well-defined personnel security policy and procedures for screening individuals before granting access to CUI as part of their CMMC compliance. However, chatting with the security guards, you discover that the contractor sometimes grants temporary access to CUI systems before completing the screening process, citing operational urgency. While examining the contractor's procedures addressing personnel screening, you expect to find the following background checks included, EXCEPT?

Health Background Checks

Criminal background and drug screening

Credit and Civil Background checks

Employment verification and education checks

The practice states that personnel security screening involves evaluating an individual's conduct, integrity, judgment, loyalty, reliability, and stability (trustworthiness) before granting access to CUI systems. While criminal, credit, civil, employment, and educational background checks are relevant for assessing trustworthiness, health background checks are not explicitly mentioned as part of the screening processes for this practice.

57.

In your assessment of an OSC?s information systems, you realize that the OSC has been having issues determining what is and isn?t CUI. One of the employees asks for your help identifying CUI so that they can take measures to protect it. They also request that you recommend a resource where they can understand the national CUI policy. Which of the following is the BEST resource they should visit to understand what CUI is and the national CUI policy?

32 CFR Part 2002 and ISOO CUI Registry

DFARS 252.204-7012 and ISOO CUI Registry

48 CFR 52.204-21 and NIST SP 800-171

22 CFR Part 120-130

The definition of CUI is provided in 32 CFR 2002.4(h) and on the ISOO Registry. Information given to the OSC by the Government or a Prime to help in the performance of a contract should be protected per the Laws, regulations, and government-wide policies. However, the OSC should ask the following questions to determine whether the information is CUI: Is the information publicly available? If yes, that is not CUI. Is the information created for the Government? Does the OSC hold or create the information on behalf of the Government? Does a Law, regulation, or government-wide policy require its handling using defined disseminating and safeguarding controls? If the answer to these questions is affirmative, then that is CUI, and they should use the DoD or the ISOO CUI registry to determine which category or subcategory it falls in and mark it appropriately.

58.

Examining an OSC password policy, you learn that a password should have a minimum of 15 characters. It also should have 3 uppercase, 2 special characters, and other alphanumeric characters. Passwords have to be changed every 45 days and cannot be easily tied to the account owner. Passwords cannot be reused until 30 cycles are complete. The OSC's systems send a temporary password to the user's email or authentication app, which is one of the events described in their password usage policy. However, a recent penetration test report shows that the generated temporary passwords did not have sufficient entropy, and an attacker may guess a temporary password through brute force attacks. Which CMMC practice has the contractor successfully implemented? Select all that apply.

IA.L2-3.5.7-? Password Complexity and IA.L2-3.5.8 ? Password Reuse

IA.L2-3.5.3 - Multifactor Authentication

IA.L2-3.5.9 - Temporary Passwords

IA.L2-3.5.6 ? Identifier Handling

The contractor's password policy meets the requirements of CMMC practice IA.L2-3.5.7-Password Complexity by defining minimum length, character types, and character change rules for passwords. The policy also meets CMMC practice IA.L2-3.5.8-Password Reuse by prohibiting password reuse until 30 password cycles are complete.

59.

You are a CCA reviewing the security measures for a defense contractor seeking CMMC Level 2 compliance. CMMC practice PE.L2-3.10.6-Alternative Work Sites requires the organization to safeguard CUI at alternate work sites, like employee home offices. You are examining their list of safeguards and the system security plan to assess their compliance. When assessing a contractor's implementation of CMMC practice PE.L2-3.10.6-Alternative Work Sites, which of the following would be the least effective method for gathering information?

Employing technologically savvy guards to man the alternate worksite

Requiring remote staff connecting to their internal networks to use a VPN that prevents split tunneling and requires multifactor authentication to verify remote users are who they claim to be

Deploying a patch management and anti-malware solution for every laptop or desktop on the alternate worksite

Using Full Disk Encryption (FDE) or Container-based encryption to encrypt CUI when stored or transmitted from or to alternate work sites

---

Employing guards is a physical security measure to secure the alternate worksite, not a technical one related to information systems. Security guards by virtue of their duties, may rarely come across CUI. Hence, No matter how technologically savvy they are, their duties will be limited to manning the physical facility.

60.

While reviewing a contractor's Microsoft Active Directory authentication policies, you observe that the account lockout threshold is configured to allow 5 consecutive invalid login attempts before locking the account for 15 minutes. Additionally, the reset account lockout counter is set to 30 seconds after each unsuccessful login attempt. To understand the contractor?s implementation of assessment objectives for AC.L2-3.1.8-Unsuccessful Logon Attempts, a CCA is required to examine all of the following EXCEPT?

Examining system developers

System security plan

Documentation on system configurations

Access control policies

AC.L2-3.1.8 requires the CCA to examine the contractor?s access control policy, procedures addressing unsuccessful logon attempts, system security plan, system design documentation, system configuration settings and associated documentation, system audit logs and records, among other relevant documents or records.

61.

After you ask to examine some audit records, the contractor's system admininstrator informs you that there is a process to follow before accessing them. The logs are hashed using SHA-512 algorithms, and the system administrator has to run an algorithm to recalculate the hashes for the audit records to verify their integrity before running a decryption algorithm to decrypt the data. Since this might take some time, you tour the facility while interviewing personnel with audit and accountability roles. You see an employee holding the door for another without using their physical access card. While interviewing the contractor's employees, you find that they can access all audit logging tools and tweak the settings according to their needs or requirements. Upon examining the contractor's access control policy, you realize they have not defined the measures to protect audit logging tools. Which of the following statements accurately describes the contractor's compliance with protecting audit logging tools from unauthorized access, modification, and deletion, as required by AU.L2-3.3.8-Audit Protection?

The contractor is not compliant, as there are no defined measures to protect audit logging tools from unauthorized access, modification, or deletion

The contractor is fully compliant; employees can access audit logging tools to meet their requirements.

The contractor is partially compliant, as audit logging tools are protected by the same measures as audit information.

The contractor's compliance cannot be determined based on the information provided.

The scenario explicitly states that upon reviewing the access control policy, there are no defined measures to protect the audit logging tools, which does not meet the requirements of CMMC practice AU.L2-3.3.8-Audit Protection. In addition, the contractor's employees, can access all audit logging tools and tweak the settings according to their needs or requirements, which is bound to introduce integrity issues in the audit logs.

62.

When examining procedures addressing system security plan development and implementation, you realize that the contractor has developed an SSP that defines and documents system boundaries. The SSP also contains the non-applicable security requirements approved by designated authorities. It also outlines other essential aspects, such as relationships with or connection to other systems, how security requirements will be implemented, etc. Upon interviewing personnel with information security responsibilities, you realize that the contractor has not reviewed or updated the SSP and has no defined timelines. How can the contractor treat practice CA.L2-3.12.4-System Security Plan in this scenario if it is found to be Not Met?

Place it in a POA&M

CA.L2-3.12.4 is not applicable for the contractor's systems.

Subcontract an RPO to help with the implementation

Negotiate with the Lead Assessor for a favorable outcome.

Because the contractor has an existing SSP that partially meets the practice, they can place the deficient areas, like defining an update frequency and implementing a review/update process, into a POA&M to satisfy CA.L2-3.12.4-System Security Plan fully over time.

63.

When assessing a contractor?s implementation of CMMC practices, you examine its System Security Plan (SSP) to identify its documented measures for audit reduction and reporting. They have a dedicated section in their SSP addressing the Audit and Accountability requirements. You proceed to interview their information security personnel, who informed you that the contractor has a dedicated Security Operations Center (SOC) and uses Splunk to reduce and report audit logs. How would you score the contractor?s implementation of AU-L2-3.3.6-Reduction & Reporting?

Met

Not Met

Not Applicable

Partially Met

The contractor has documented measures for audit reduction and reporting in its System Security Plan (SSP), and it has a dedicated Security Operations Center (SOC) that uses Splunk for audit log reduction and reporting. Splunk is a widely used Security Information and Event Management (SIEM) tool that can effectively handle audit log reduction and reporting requirements.

64.

A defense contractor retains your services to assess their information systems for CMMC compliance, particularly configuration management. The contractor uses CFEngine 3 for automated configuration and maintenance of its computer systems and networks. While chatting with the network?s system admins, you realize they have deployed a modern compliance checking and monitoring tool. However, when examining their configuration management policy, you notice the contractor uses different security configurations than those recommended by product vendors. The system administrator informs you they do this to meet the minimum configuration baselines required to achieve compliance and align with organizational policy. When examining the contractor's security configuration checklists, which of the following parameters are you not likely to find?

The contractor's assessment readiness status

Network configuration and port management

File and Directory permissions

Protocol usage and application allowlisting

When examining security configuration checklists or guidelines, you will likely find settings related to various security parameters, including network configuration and port management, file and directory permissions, protocol usage and application allowlisting, registry settings, account settings, and remote connection settings. These parameters impact the security posture of the systems and should be configured according to the organization?s security requirements and industry best practices. The contractor's assessment readiness status is not something you will find in the security configuration checklists; rather the results of the assessment readiness reivew, will be documented on the Certification Assessment Readiness Review (CA-RR) checklist.

65.

During your assessment of Defcon's (a contractor) implementation of CMMC Level 2 practices, you notice that their system for displaying security and privacy notices is insufficient. The banners currently in use lack detailed information about Controlled Unclassified Information (CUI) handling requirements and associated legal implications. Additionally, the banners are not consistently displayed across all contractor systems and workstations. Moreover, the banners on login pages disappear automatically after less than 5 seconds, providing insufficient time for users to read and acknowledge the content. Which of the following is NOT a feature Defcon's Systems updated privacy and security notices should have?

Display duration set to less than 5 seconds before automatically disappearing

A general statement about monitoring and recording of system usage

Specific information about the presence of CUI and associated handling requirements

A warning about unauthorized use being subject to civil and criminal penalties

---

The contractor should fully implement the requirements of CMMC practice AC.L2-3.1.9-Privacy & Security Notices to ensure that its employees are fully informed of their CUI handling obligations.

66.

An OSC has an established Incident Response plan and a dedicated team specifically trained to handle any potential incidents and conduct necessary analysis. When performing the assessments, you also realize the OSC has deployed IDS and SIEM tools to identify possible incidents. Examining the Contractor's incident response policy, you also learn they have defined and implemented containment strategies and have developed clear procedures for system and data recovery after an incident, including backup and restore procedures. There is also a communication protocol in place to inform the affected stakeholders and users after a security incident. Chatting with a few members of the OSC's incident response team, you learn they conduct regular drills to test and improve the effectiveness of the incident-handling capability. There also are defined and documented incident response mechanisms and a post incident analysis procedure to identify lessons learned and make necessary improvements to the incident-handling process. Based on the information provided, how would you assess the OSC's compliance with the IR.L2-3.6.1-Incident Handling practice?

Met (+5 points)

Not Met (-5 point)

Not Met (-1 point)

Met (+1 point)

Based on the comprehensive measures described in the scenario, including an established incident response plan, dedicated team, detection tools, containment strategies, recovery procedures, communication protocols, regular drills, and post-incident analysis, the OSC's compliance with CMMC practice IR.L2-3.6.1-Incident Handling should be scored as Met (+5 points).

67.

In assessing an OSC's CUI handling practices, you learn they use an approved algorithm (AES-256) to encrypt the data to ensure its confidentiality. However, the encryption module they are using has not been validated under the FIPS 140 standard. The OSC believes that using an approved algorithm is sufficient to comply with the CMMC practice for CUI encryption requirements. Where can you find information about a cryptographic module?s current status with FIPS?

NIST CMVP

FIPS 140-2 documentation

FedRAMP Marketplace

NIST CSRC

For CMMC practice SC.L2-3.13.11-CUI Encryption, the OSC?s claim that the product is FIPS-validated must be substantiated with evidence. When encryption is employed, the module must comply with FIPS 140-2. Evidence of a product's current FIPS status can be found on NIST's Cryptographic Module Validation Program website.

68.

A contractor is preparing to bid on an upcoming DoD contract to provide next-generation upper limb prosthetics for injured servicemen. Part of the preparation is undergoing a CMMC assessment, and they have hired you to assess their implementation of CMMC practices. The contractor has multiple design, manufacturing, and supply chain management systems. Each system generates its audit logs, which are stored in separate repositories. Different teams analyze and review them independently, with each team reporting the findings to the respective departmental heads. For instance, the engineering team reviews and analyzes logs related to the design systems and reports to the lead engineer, while the operations team focuses on the manufacturing system logs. When interviewing personnel responsible for audit record review, analysis, and reporting, they inform you that this is deliberately set up to ensure departmental independence and granular risk identification. Based on the CMMC practice AU.L2-3.3.5-Audit Correlation, what is the likely issue you would identify with the contractor's current approach?

The audit review, analysis, and reporting processes are not correlated across systems

Lack of defined processes for audit record review, analysis, and reporting

Failure to retain audit logs for an adequate duration

Absence of automated mechanisms for analyzing and correlating audit records

---

While audit logs are generated and reviewed, there is no centralized process for correlating these logs across different systems within the contractor's organization, which goes against the requirements of CMMC practice AU.L2-3.3.5-Audit Correlation. The audit record review, analysis, and reporting should be correlated at the system or departmental level to ensure they operate collectively.

69.

A defense contractor handles sensitive Controlled Unclassified Information (CUI) and has implemented strict policies and controls for using portable storage devices containing CUI on external systems. Their Information Security Policy outlines approved encrypted devices and defines circumstances for their limited use on external systems with prior approval. The approval process requires documenting the need, external systems involved, and data protection measures. All approved portable storage devices use FIPS 140-2 validated encryption and can only be unlocked on the contractor's internal or authorized external systems with proper authentication. Based on this scenario, has the contractor met all the assessment objectives for CMMC practice AC.L2.3.1.21-Portable Storage Use?

Yes, the contractor has met all the assessment objectives

No, the contractor has Not Met the assessment objectives

The contractor has partially met the assessment objectives

It is unclear based on the scenario

Based on the details provided in the scenario, it appears the contractor has met all the assessment objectives for CMMC practice AC.L2-3.1.21-Portable Storage Use. 1) The use of portable storage devices containing CUI on external systems is identified and documented: The scenario states that the contractor's Information Security Policy outlines the approved types of portable storage devices that can be used, and their use on external systems must be explicitly approved and documented, including the business need and specific external systems involved. 2) Limits on the use of portable storage devices containing CUI on external systems are defined: The policy defines the circumstances and limitations for using portable storage devices on external systems, such as requiring approval, encryption, and proper authentication/access controls. 3) The use of portable storage devices containing CUI on external systems is limited as defined: The scenario mentions that the contractor has implemented technical controls to enforce the policy, allowing the approved encrypted portable devices to be used only on the contractor's internal systems or authorized external systems with proper authentication. Therefore, based on the information provided, it seems the contractor has addressed all three assessment objectives for AC.L2-3.1.21-Portable Storage Use, by identifying and documenting the use cases, defining limits and restrictions, and technically limiting the use of portable storage devices containing CUI on external systems as per their defined policy.

70.

After a security audit, a contractor documents specific vulnerabilities and deficiencies in an audit report. After examining its POA&M, you realize it has a clearly defined policy on addressing these deficiencies and by when. However, after interviewing the contractor?s security and compliance team, you learn that while an audit is regularly conducted, the remediating measures are not always taken, and when taken, they are not always practical. The security and compliance team informs you they have tried reaching the system administrator to explain the repercussions of this without success. Based on the scenario, how would you rate the contractor?s implementation of CA.L2-3.12.2-Plan of Action?

Not Met

Met

Not Applicable

Partially Met

Since a core aspect of developing and implementing an effective plan of action to correct deficiencies is falling short, the overall practice cannot be considered fully met based on the evidence provided. The contractor has documented plans and policies but is failing in the execution of these plans. The fact that remediation efforts are inconsistent and not always practical suggests that the contractor is not fully meeting the requirements of CA.L2-3.12.2-Plan of Action. The lack of effective follow-up and resolution of the issues further supports a rating that indicates the contractor's implementation is inadequate. Here's the rationale: Policy and Documentation: The contractor has a clearly defined policy on addressing deficiencies and deadlines documented in the Plan of Action & Milestones (POA&M). This is a positive aspect, indicating that the contractor has formal processes in place for identifying and planning the remediation of security vulnerabilities. Execution and Practicality: Despite having a POA&M and a regular audit process, the contractor is failing to effectively execute the remediation measures. The scenario indicates that the necessary actions are either not being taken, or when they are, they are not practical or effective. This suggests a significant gap between the policy (what should happen) and practice (what is actually happening). Communication and Follow-Up: The security and compliance team has identified the issues and attempted to address them by communicating with the system administrator, but these efforts have not been successful. This indicates a breakdown in communication or a lack of accountability within the organization, further undermining the effectiveness of the POA&M. Overall Assessment: The core requirement of CA.L2-3.12.2 is to establish and maintain plans of action to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. The contractor has established these plans

but has not maintained them effectively, as the deficiencies are not being practically or consistently addressed.

71.

During a CMMC assessment for an OSC, the CCA needs to assess their implementation of CMMC practice MP.L2-3.8.4-Media Markings, which requires proper marking and labeling of CUI. The interview with the information security personnel reveals a well-defined policy, but you need concrete evidence to verify its effectiveness. Which of the following would provide sufficient evidence to assess a contractor's implementation of CMMC practice MP.L2-3.8.4-Media Markings?

Reviewing a sample of media containing CUI for proper markings and labelling

Interviewing personnel responsible for information security.

Observing the physical security controls in designated controlled areas.

Examining the organization's system security plan.

While interviewing personnel responsible for information security or examining the organization's SSP may give some insights, reviewing the sample media containing CUI for proper markings and labelling would meet both adequacy and sufficiency metrics to assess the OSC's implementation of CMMC practice MP.L2-3.8.4-Media Markings.

72.

An engineering company works on DoD contracts that involve handling CUI. They use hardcopy media such as printed paper, microfilms, and digital media, including flash drives, SSDs, DVDs, and internal and external hard drives. During a CMMC assessment, you discover the engineering company has defined procedures addressing media storage and access governed by an access control policy. All media containing CUI is marked and stored in biometrically locked cabinets. To store CUI on digital media, an authorized user must be identified using their biometrics or authenticated using an integrated MFA solution. To access non-digital media, the user must be on a defined list of authorized personnel and sign three forms. You also learn that the contractor maintains a comprehensive inventory of all CUI media. The scenario describes a multi-factor authentication (MFA) solution being used to access digital media containing CUI. However, the access control procedures for non-digital media require authorized personnel to sign three separate forms. While both methods aim to verify user identity, which of the following is the MOST significant security concern associated with the reliance on a paper-based form process?

The forms are susceptible to forgery, resulting in unauthorized access.

It can be time-consuming to complete the forms for frequent access.

The paper forms cannot be easily integrated with other security systems.

It requires users to memorize more information for access.

Paper-based forms can be forged or tampered with, potentially allowing unauthorized individuals to gain access to sensitive CUI media. This vulnerability is more concerning than the time-consuming nature of the process, lack of integration with other security systems, or the need to memorize information, as it directly impacts the integrity of access control. MFA provides a more robust security control by requiring additional verification factors beyond just knowledge (e.g., something you have, something you are).

73.

You are a CCA reviewing the security measures for a defense contractor seeking CMMC Level 2 compliance. CMMC practice PE.L2-3.10.6-Alternative Work Sites requires the organization to safeguard CUI at alternate work sites, like employee home offices. You are examining their list of safeguards and the system security plan to assess their compliance. When assessing a contractor's implementation of CMMC practice PE.L2-3.10.6-Alternative Work Sites, which of the following would be the least effective method for gathering information?

Interviewing personnel with information security responsibilities

Testing the actual security controls employed at alternate work sites

Examining procedures addressing alternate work sites for personnel

Reviewing assessments of safeguards at alternate work sites

While interviews can provide valuable insights, they rely on the personnel's knowledge and recollection, which may not be fully reliable, comprehensive or up-to-date regarding the specific controls and monitoring for alternate work sites. Reviewing assessments of safeguards at alternate work sites would provide direct evidence of the security posture and implemented controls at those sites. On the other hand, reviewing documented procedures is crucial to verifying the existence and requirements for alternate work site controls. Hands-on testing would be the most reliable method to validate the implementation and effectiveness of the required controls.

74.

During your review of an OSC?s system security control, you focus on CMMC practice SC.L2-3.13.9-Connections Termination. The OSC uses a custom web application for authorized personnel to access CUI remotely. Users log in with usernames and passwords. The application is hosted on a dedicated server within the company?s internal network. The server operating system utilizes default settings for connection timeouts. Network security is managed through a central firewall, but no specific rules are configured for terminating inactive connections associated with the CUI access application. Additionally, there is no documented policy or procedure outlining a defined period of inactivity for terminating remote access connections. Interviews with IT personnel reveal that they rely solely on users to remember to log out of the application after completing their work. The scenario describes using a central firewall for network security. How could the firewall be configured to help achieve the objectives of CMMC practice SC.L2-3.13.9-Connections Termination, for the remote access application?

Creating firewall rules to identify and terminate connections associated with the CUI access application that have been inactive for a predefined period.

Encrypting all traffic between the user device and the server to protect CUI in transit.

Implementing intrusion detection and prevention systems (IDS/IPS) to identify and block suspicious activity on the server.

Blocking all incoming traffic to the server hosting the CUI access application, except from authorized IP addresses.

Firewalls can be configured with specific rules to manage connections and enforce timeouts. In this scenario, the OSC can create firewall rules to identify connections associated with the CUI access application and terminate them after a predefined period of inactivity, thus aligning with CMMC practice SC.L2-3.13.9-Connections Termination.

75.

When assessing a contractor?s implementation of CMMC practices, you examine its System Security Plan (SSP) to identify its documented measures for audit reduction and reporting. They have a dedicated section in their SSP addressing the Audit and Accountability requirements. You proceed to interview their information security personnel, who informed you that the contractor has a dedicated Security Operations Center (SOC) and uses Splunk to reduce and report audit logs. What assessment method would you use in evaluating CMMC practice AU.L2-3.3.6-Reduction & Reporting?

Testing

Evaluating

Examining

Interviewing

NIST SP 800-171A defines the "Test" assessment method as exercising assessment objects under specific conditions to compare actual and expected behaviors and evaluating security control effectiveness. The "Examine" method involves reviewing and analyzing to determine if security controls are implemented and operating correctly. To evaluate Splunk's audit reduction and report generation capabilities, particularly for CMMC practice AU.L2-3.3.6-Reduction & Reporting, the "Test" assessment method is the best method to use in this scenario and is preferred over "Examine." Testing Splunk under various conditions with sample logs allows for a hands-on evaluation of log processing, reduction, and reporting, ensuring a comprehensive assessment of security control effectiveness by comparing actual outputs with expected outcomes. This approach provides a more thorough understanding of the system's capabilities than merely examining configurations or outputs.

76.

When assessing an OSC, you learn they have implemented several measures to protect the authenticity of their communications. All information marked CUI is encrypted using a FIPS-validated cryptographic module to ensure its confidentiality. In discussions with the system administrators, you find they use certificate-based authentication to verify the identities of communicating parties. The authenticity of digital files is verified using SHA-256 hashes. The OSC also produces logs of communication sessions to track and verify activity as evidence of compliance with SC requirements. How would you score the contractor?s implementation of CMMC practice SC.L2-3.13.15-Communications Authenticity based on this scenario?

Met

Not Met

Not Applicable

Partially Met

CMMC practice SC.L2-3.13.15-Communications Authenticity focuses on ensuring that a trust relationship is established between communication parties, which directly relates to communication authenticity. The scenario describes measures such as encryption for CUI confidentiality, certificate-based authentication to verify the identities of communicating parties, and SHA-256 hashing to verify file integrity?all of which strengthen authenticity. Based on these implemented measures supporting authenticity, the OSC deserves a 'MET' score on the SPRS.

77.

During a CMMC assessment, you need to verify how a defense contractor protects sensitive data on storage devices. CMMC practice SC.L2-3.13.16-Data at Rest, specifically focuses on this requirement. What is the main requirement of CMMC practice SC.L2-3.13.16-Data at Rest?

Ensuring CUI confidentiality while at rest.

Control and monitor the use of VoIP technologies.

Protect the confidentially of CUI at backup storage locations.

Implementing access control measures for CUI storage devices.

CMMC practice SC.L2-3.13.16-Data at Rest, focuses on protecting Controlled Unclassified Information (CUI) at rest within the organization's information systems. It ensures that unauthorized individuals cannot access or view CUI.

78.

You are assessing an OSC that develops applications handling Controlled Unclassified Information (CUI). As part of the assessment, you review their vulnerability scanning process. According to their risk assessment policy, the OSC conducts system vulnerability scans every three months. However, they also utilize a centralized, automated vulnerability scanning tool that performs daily scans. Upon discovering any vulnerabilities, the OSC?s team applies patches and rescan their systems. Their environment includes backend database servers, web applications with custom Java code, virtual machine hosts running containerized applications, network firewalls, routers, switches, and developer workstations. During the assessment, you find that their scanning solution integrates the latest vulnerability feeds from the National Vulnerability Database (NVD), Open Vulnerability and Assessment Language (OVAL), and vendor sources. The tool generates reports using Common Vulnerability Scoring System (CVSS) metrics, and even remotely connected developer laptops are included in the scans. However, upon reviewing the vulnerability reports, you observe that the same high/critical vulnerabilities persist month after month without evidence of remediation. Furthermore, there is no record of source code scanning for their custom applications, and virtual machine hosts running the containerized applications are not included in the scans. To fully remediate the finding about containers being missed by vulnerability scans, which additional step would be required?

Ensure that the vulnerability scanning tool is configured to include virtual machine hosts and containerized environments in its scans, and rebuilding/redeploying containers.

Deploy a separate specialized container scanning solution

Implement runtime application self-protection (RASP) for containerized applications

Engage a third-party penetration testing firm to assess the containerized environment

---

To fully remediate the finding that vulnerability scans are missing containers, two steps are required. First, the existing vulnerability scanning solution needs to be reconfigured to ensure virtual machine hosts and containerized environments in its scans. This involves updating the scanning tool?s configuration or employing a specialized scanning tool that can assess both the host systems and the containers they run. However, this alone does not address potentially vulnerable containers already deployed. Therefore, the second step of rebuilding all containers from trusted base images after being scanned and then redeploying them is also needed. Both steps are required for full remediation and would allow the OSC to detect and

address vulnerabilities within the containers and their underlying infrastructure, ensuring comprehensive coverage of the entire environment.

79.

After a security audit, a contractor documents specific vulnerabilities and deficiencies in an audit report. After examining its POA&M, you realize it has a clearly defined policy on addressing these deficiencies and by when. However, after interviewing the contractor?s security and compliance team, you learn that while an audit is regularly conducted, the remediating measures are not always taken, and when taken, they are not always practical. The security and compliance team informs you they have tried reaching the system administrator to explain the repercussions of this without success. When examining the contractor?s plan of action, you expect to find all the following, EXCEPT?

The guilty party for introducing the deficiency or vulnerability

Ownership of who is accountable for ensuring the plan?s performance

Specific clear and actionable steps or milestones, including completion dates

Milestones to measure plan progress and assign responsibility for each step or milestone

---

The Plan of Action & Milestones (POA&M)focuses on defining the steps and milestones to resolve or mitigate identified issues. While it may indicate the source system or root cause in some cases, explicitly calling out individuals responsible for introducing a deficiency is not an expected component. The POA&M is a forward-looking plan, not an assessment of guilt.

80.

When assessing a contractor?s implementation of CMMC requirements, you realize they have multiple data centers and regional offices, each having its access control mechanisms and security perimeter. The contractor uses a remote access solution to allow external partners and employees to collaborate on projects that involve CUI. The solution requires routing configuration to ensure the remote access to CUI is not compromised. In assessing the contractor's implementation of AC.L2-3.1.14- Remote Access Routing, what must you determine?

Managed access control points are identified, implemented, and remote access is routed through these managed network access control points.

The contractor manages access control points

All remote access is monitored

All users are authenticated before being granted remote access.

AC.L2-3.1.14-Remote Access Routing identifies two assessment objectives and requires the assessor to determine if: [a] managed access control points are identified and implemented; and [b] remote access is routed through managed network access control points.

81.

CMMC practice PS.L2-3.9.1-Screen Individuals, requires individuals to be screened before authorizing access to organizational systems containing CUI. However, in the assessment you are currently conducting, there is no physical evidence confirming the completion of personnel screens, such as background checks, only affirmations derived from an interview session. In an interview with the HR Manager, they informed you that before an individual is hired, they submit their information through a service that performs criminal and financial checks. How would you score the OSC's implementation of CMMC practice PS.L2-3.9.1-Screen Individuals, objective [a]?

More information is needed.

Not Met

Not Applicable

Met

Affirmations are acceptable evidence provided they support the Assessment Objectives and the information is derived from someone responsible for the process (such as an HR Manager responsible for conducting the screening) or someone who is a subject of the process (e.g., an employee with access to CUI who can verify that their background check was performed prior to gaining network access). However to verify and support what the HR Manager and/or employee claim, physical evidence, in the form of records of previous personnel screens (background checks) should be provided to addresses the intent of PS.L2-3.9.1[a] individuals are screened prior to authorizing access to organizational systems containing CUI.

82.

CMMC MA.L2-3.7.6-Maintenance Personnel, requires that maintenance personnel without required access authorization be supervised during maintenance activities. One of the ways organizations can achieve this is to develop a documented procedure for supervised maintenance activities. Which of the following elements should be excluded from the documented procedure?

A detailed list of all CUI assets that the maintenance activity might impact.

The specific steps authorized for the visiting maintenance personnel with limited access

The method used to authenticate and monitor the supervisor's activity during the maintenance session.

Contact information for the organization's IT security team in case of emergencies or unexpected issues.

A detailed list of all CUI assets that the maintenance activity might impact is unnecessary for the documented procedure. The focus should be on the tasks performed, not the potentially impacted CUI assets (which might change based on the specific maintenance). The other answer options all directly address elements crucial for supervised maintenance, according to MA.L2.3.7.6--Maintenance Personnel.

83.

When examining a contractor's security configuration settings, you find they have thoroughly documented the essential ports, protocols, services, and programs required for their business operations. They follow industry security configuration standards, such as CIS Benchmarks, to ensure systems are securely configured and hardened. Interviewing the network administrator and reviewing their processes, you learn that the contractor has implemented a rigorous whitelisting approach to control the execution of programs on their systems. Only applications and services that are deemed necessary for the system's function are explicitly allowed to run and are tightly controlled. They use Secure File Transfer Protocol (SFTP) services on port 22, Simple Mail Transfer Protocol (SMTP) on port 25, and DNS services on port 53, while restricting all other unnecessary ports and services using robust firewall configurations. The contractor conducts regular reviews of system services and functionalities to identify and disable any nonessential components that may have been inadvertently enabled or introduced through software updates or changes. They maintain a comprehensive inventory of all approved software, ports, protocols, and services, which is regularly audited and reconciled against the actual system configurations. How would you score the contractor's implementation of CM.L2-3.4.7-Nonessential Functionality?

Met (+5 points)

Not Met (-1 point)

Met (+1 point)

Not applicable

The scenario demonstrates that the contractor has implemented comprehensive measures to identify, document, and actively manage essential functionality while restricting or turning off nonessential components as required by CMMC practice CM.L2-3.4.7-Nonessential Functionality. They have thoroughly addressed all the assessment objectives outlined in the practice and thus it can be scored as Met.

84.

Organizations have to control what systems can be installed for the principle of least functionality to apply. You assess the contractor's implementation of Configuration Management requirements and start by examining their documentation. They maintain a regularly updated inventory of authorized software to support their allowlisting and blocklisting efforts. The contractor has configured their information systems such that only authorized software can be executed or installed after software approval. Any attempts to install unauthorized software by unauthorized personnel are automatically logged, and an alert is sent to the system administrator. How would you rate the contractor's implementation of CM.L2-3.4.8-Application Execution Policy?

Met (+5 points)

Met (+1 point)

Not Met(-5 points)

Not Met (-1 point)

The contractor has implemented measures that fully satisfy the requirements of CM.L2-3.4.8-Application Execution Policy. They maintain an up-to-date inventory of authorized software, configure their systems to allow only authorized software to execute or install, and establish a software approval process. Additionally, any attempts to install unauthorized software are logged, and alerts are sent to the system administrator, demonstrating effective monitoring and control.

85.

In preparation for a CMMC Level 2 assessment, an OSC must ensure their CUI handling practices are fully compliant with the laws, regulations, and government-wide policies. The OSC employee should acquaint themselves with the following Laws, Regulations, or Government Wide Policies EXCEPT?

Executive Order 13526 and Regulatory Authority: 48 CFR 52.204-21

Regulatory Authority: 32 CFR Part 2002, Controlled Unclassified Information (CUI)

Legal authorities: 2002 Federal Information Security Management Act (FISMA) Amended in 2014 and Executive Order 13556, Controlled Unclassified Information

Policy: National Archive & Records Administration (NARA) Information Security Oversight Office (ISOO) CUI Notices

---

FISMA establishes guidelines and security standards to protect sensitive government information and operations. Such information includes CUI and FCI. However, Executive Order 13556 standardized how unclassified information should be protected, leading to the establishment of 32 CFR 2002 as the regulation governing Controlled Unclassified Information (CUI). The regulation established a CUI Executive Agent (EA), which NARA delegated to the ISOO Director. The EA maintains the CUI registry and issues regular notices considered federal policy.

86.

A defense contractor retains your services to assess their information systems for CMMC compliance, particularly configuration management. The contractor uses CFEngine 3 for automated configuration and maintenance of its computer systems and networks. While chatting with the network?s system admins, you realize they have deployed a modern compliance checking and monitoring tool. However, when examining their configuration management policy, you notice the contractor uses different security configurations than those recommended by product vendors. The system administrator informs you they do this to meet the minimum configuration baselines required to achieve compliance and align with organizational policy. Based on your understanding of the CMMC Assessment Process, how would you score CM.L2-3.4.2-Security Configuration Enforcement if the contractor is tracking it in a POA&M?

Not Met

Not Applicable

Met

Need more information to score this practice.

According to the CMMC Assessment Process (CAP), any practice being tracked or placed in a POA&M should be scored as Not Met. This status can only be changed during the POA&M Closeout Assessment and if the requirements of the POA&M Closeout Assessment are fully met. Regardless, however, CM.L2-3.4.2-Security Configuration Enforcement cannot be placed in a POA&M as it does not meet the criteria set out in the Limited Practice Deficiencies section of the CAP.

87.

You are assessing a contractor?s implementation for CMMC practice MA.L2-3.7.4-Media Inspection, by examining their maintenance records. You realize the maintenance logs identify a repeating problem. A recently installed central server has been experiencing issues affecting the performance of the contractor?s information systems. This is confirmed by your interview with the contractor?s IT team. You requested to investigate the server, and the IT team agreed. On the server, there is a file named conf.zip that gets your attention. You decide to open the file in an isolated computer for further review. To your surprise, the file is a .exe used when testing the server for data exfiltration. How should this incident be handled?

In accordance with the incident response plan

By sandboxing the malicious code and continuing with business as usual

Decommissioning the server and installing a new one

By immediately reporting it to the FBI's Cyber Division

CMMC practice MA.L2-3.7.4-Media Inspection requires that after determining whether the media contains test and diagnostic programs, such incidents should be handled in a manner consistent with the organization?s incident handling process and procedures, by following these steps: Verify the Incident: Confirm that the presence of the malicious .exe file is an actual security incident and not a false positive. Assess the Scope: Determine whether the issue is isolated to the central server or if other systems may be compromised as well. Immediate Containment: Isolate the affected server from the network to prevent further data exfiltration or lateral movement of the malicious software. Remove the Malicious File: Identify and remove the .exe file and any other malicious software or files on the server. Investigate the Root Cause: Determine how the malicious file was introduced, whether through a maintenance procedure or another vulnerability. Restore the System: Ensure the server is clean, and then restore it to normal operation using verified backups or a clean image. Verify Integrity: Ensure that all systems connected to the server are checked for any signs of compromise and that they are secure before bringing the server back online. Review Logs and Documentation: Analyze the server and network logs to gather more information about the incident, such as the timeline of events and the method of infiltration. Conduct a Root Cause Analysis: Document the findings and determine what led to the incident, including any failures in policies or controls.

88.

Examining an OSC?s system design documentation, you notice they have implemented a CUI enclave and have a documented procedure addressing boundary protection. They have segmented their network into different zones, each having its own rules to allow or deny traffic. The OSC has implemented strict firewall rules that deny all incoming and outgoing traffic by default, only allowing specific traffic as required. To automatically block unrecognized traffic patterns, the OSC has provisioned a state-of-the-art Intrusion Detection and Prevention System (IDPS). During an interview with the network administrator, you realize that OSC uses a whitelisting approach to explicitly allow only certain IP addresses, domains, or services to communicate with their system. Their IT security team monitors network traffic to detect any unauthorized attempts to connect or communicate with their system. The scenario states that network traffic is monitored to detect unauthorized connection attempts. Based on the scenario and your understanding of the CMMC scoring methodology, how would you score the OSC?s implementation of CMMC practice SC.L2-3.13.6-Network Communication by Exception?

Met (5 points)

Met (1 point)

Met (3 points)

Not applicable

From the scenario, the OSC has demonstrated that network communications traffic is denied by default [a] and is only allowed by exception based on explicit rules and whitelisting [b]. The examined documentation, security controls, and monitoring processes provide evidence that the practice has been adequately implemented, which justifies a score of 5 points on the assessment.

89.

Change is a part of any production process and must be meticulously managed. System Change Management is a CMMC requirement, and you have been called in to assess the implementation of CMMC requirements. When examining the contractor?s change management policy, you realize there is a defined change advisory board that has a review and approval mandate for any proposed changes. The change advisory board maintains a change request system where all the changes are submitted and documented for easy tracking and review. The contractor also has a defined rollback plan defining what to do in case the approved changes result in unexpected issues or vulnerabilities. What evidence artifacts can the contractor also cite as evidence to show their compliance with CM.L2-3.4.3-System Change Management besides their compliance management policy?

Organizational procedures addressing system configuration change control and change control/audit review reports

Antivirus scan reports detailing detected and quarantined threats.

System uptime statistics showing improved stability after change management implementation.

Employee satisfaction surveys regarding the change management process.

The contractor can cite many evidence artifacts, including its procedures for addressing system configuration change control, minutes or agendas from change control oversight meetings, personnel knowledge of their roles in system change management, etc.

90.

While reviewing a contractor's Microsoft Active Directory authentication policies, you observe that the account lockout threshold is configured to allow 5 consecutive invalid login attempts before locking the account for 15 minutes. Additionally, the reset account lockout counter is set to 30 seconds after each unsuccessful login attempt. What specific threat is this configuration designed to mitigate?

Brute Force attacks

Spoofing attacks

Ransomware attacks

Phishing attacks

Attackers use automated tools to systematically try multiple username and password combinations to gain unauthorized access to a system or network. The reset counter mechanism ensures that after each unsuccessful login attempt, the lockout threshold does not quickly reach its limit. This makes it more difficult for an attacker to rapidly attempt multiple password guesses in a short period. By resetting the counter after each failed attempt, it forces an attacker to spread their attempts over a longer period, reducing the likelihood of success before the account is locked. This way the contractor can mitigate the risk of a brute force attack by limiting the number of unsuccessful login attempts allowed before locking the account and providing a delay period before allowing further login attempts.

91.

You are assessing an OSC that uses various collaborative computing devices, such as video conferencing systems, networked whiteboards, and webcams, for remote meetings and presentations. During your assessment, you examine the OSC?s collaborative device inventory and find that they have identified and documented all collaborative computing devices. Most of the identified devices have indicators (e.g., LED lights) that notify users when the devices are in use. The OSC has also implemented a policy prohibiting the remote activation of collaborative computing devices without user consent. However, you find that the web cameras can be activated remotely by authorized IT personnel for troubleshooting purposes. In addition to interviewing personnel, what other evidence would be helpful to assess the OSC?s compliance with CMMC practice SC.L2-3.13.12-Collaborative Device Control regarding the remote activation of web cameras? Choose all that apply.

A documented risk assessment that identifies the potential risks associated with remote camera activation and outlines mitigation strategies.

System configuration settings for the web cameras, verifying that remote activation is enabled.

User training records indicating that employees are aware of the policy and understand the potential consequences of unauthorized remote camera activation.

Network traffic logs showing no instances of remote activation attempts on the web cameras.

The OSC can also produce a risk assessment demonstrating that it has considered the security risks of remote activation and outlined mitigation strategies, including the rationale for granting IT this access. Additionally, the assessor can examine system configuration settings to verify that technical controls are in place. This ensures that remote activation is disabled for everyone except authorized IT personnel, aligning with the documented exception and mitigating the identified risk.

92.

When assessing a contractor?s implementation of CMMC requirements, you realize they have multiple data centers and regional offices, each having its access control mechanisms and security perimeter. The contractor uses a remote access solution to allow external partners and employees to collaborate on projects that involve CUI. The solution requires routing configuration to ensure the remote access to CUI is not compromised. Why should all traffic be routed through a managed Access Control point?

Reduces the susceptibility to unauthorized access to organizational systems

It provides better performance and lower latency for remote users.

It enables easier troubleshooting and monitoring of network traffic.

It simplifies network architecture and reduces complexity.

Routing all the traffic via a managed access control point allows the contractor to control remote connections, reducing a network?s susceptibility to unauthorized access. By setting up and securing the managed access control points, the organization also reduces the attack surface while simplifying the network management, allowing for better monitoring and control of all remote connections.

93.

You have been sent to assess an OSC?s implementation of CMMC practices, one of which is AC.L2-3.1.11-Ssession Termination. You expect to find the following items when examining the contractor?s list of conditions or trigger events requiring session termination, EXCEPT?

Pre-approved user activity for specific functionalities

Organization-defined periods of user inactivity

Targeted responses to certain types of incidents

Time-of-day restrictions on system use

The list of conditions or trigger events requiring session disconnect should include all the events that could trigger a session termination. These may include detected malicious activities, an organizationally defined period of user inactivity, day or time restrictions, predefined timeouts for specific functionalities, Multiple failed login attempts, etc.