2026

CMMC Level 2 Assessment Scope

(Main Reference: DoD-CIO-00003 (ZRIN 0790-ZA19) and DoD-CIO-00006 (ZRIN 0790-ZA22) Version 2.13 | September 2024 (Latest version)

AMANDA PAGE

This Assessment is based on Version 2 to correlate with current NIST / SPRS Scoring assessments.

Table of Contents

What to Include

Asset Categories

For a Level 2 assessment, assets are mapped into one of five categories[1]

Controlled Unclassified Information (CUI) Assets

1) Description:
   a) CUI Assets process, store, or transmit CUI as follows:
      i) Process – CUI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed).
      ii) Store – CUI is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents).
      iii) Transmit – CUI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).
2) Your Requirements
   a) Document in the asset inventory
   b) Document asset treatment in the System Security Plan (SSP)

[1] 32 CFR § 170.19(c)(1)

c) Document in the network diagram of the CMMC Assessment Scope
d) Prepare to be assessed against CMMC Level 2 security requirements

3) CMMC Assessment Requirements:
   a) Assess against all Level 2 security requirements

Security Protection Assets/Security Protection Data

1) Description:
   a) Assets that provide security functions or capabilities to your CMMC Assessment Scope and include Security Protection Data.
      i) Security Protection Data is security-relevant information which, if disclosed, could aid an attacker in the compromise of the system. It includes, but is not limited to:
         (1) configuration data required to operate a security protection asset,
         (2) log files generated by or ingested by a security protection asset,
         (3) data related to the configuration or vulnerability status of in-scope assets, and
         (4) passwords that grant access to the in-scope environment.
   b) People – may include but not limited to,
      i) Consultants who provide cybersecurity service
      ii) Managed service provider personnel who implement system maintenance
      iii) Enterprise network administrators
   c) Technology – May include, but are not limited to,
      i) servers,
      ii) client computers,
      iii) mobile devices,
      iv) network appliances (e.g., firewalls, switches, APs, and routers),
      v) VoIP devices,
      vi) applications,
      vii) virtual machines, and
      viii) database systems.
   d) Facilities – May include, but are not limited to,
      i) physical office locations,
      ii) satellite offices,
      iii) server rooms,
      iv) datacenters,
      v) manufacturing plants, and
      vi) secured rooms.
   e) External Service Provider (ESP) –means external people, technology, or facilities that you utilize for provision and management of comprehensive IT and/or cybersecurity services.[2]
2) Your Requirements:

[2] 32 CFR § 170.4

a) Document in the asset inventory
b) Document asset treatment in SSP
c) Document in the network diagram of the CMMC Assessment Scope
d) Prepare to be assessed against CMMC Level 2 security requirements

3) CMMC Assessment Requirements:
   a) Assess against Level 2 security requirements that are relevant to the capabilities provided

Contractor Risk Managed Assets

1) Description:
   a) Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
   b) Assets are not required to be physically or logically separated from CUI assets
   c) Contractor Risk Managed Assets are not required to be physically or logically separated from CUI Assets.
2) Your Requirements:
   a) Document in the asset inventory
   b) Document asset treatment in the SSP
   c) Document in the network diagram of the CMMC Assessment Scope
   d) Prepare to be assessed against CMMC Level 2 security requirements
3) CMMC Assessment Requirements:
   a) Review the SSP:
      i) If sufficiently documented, do not assess against other CMMC security requirements, except as noted
      ii) If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies
      iii) The limited check(s) shall not materially increase the assessment duration nor the assessment cost
      iv) The limited check(s) will be assessed against CMMC security requirements

Specialized Assets

1) Description:
   a) Assets that can process, store, or transmit CUI but are unable to be fully secured. [3]

      Examples:
      Internet of Things (IoT) devices and Industrial Internet of Things (IIoT) devices : may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors[4]

[3] 32 CFR § 170.19(c)(1)
[4] NIST SP 800-172A

Operational Technology (OT): includes industrial control systems, building management systems, fire control systems, and physical access control mechanisms.[5]
Government Furnished Equipment (GFE): includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification.[6][7]
Restricted Information Systems: means systems [and associated Information Technology (IT) components comprising the system] that are configured based entirely on government security requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).
Test Equipment: means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables.

1) Your Requirements:
   a) Document in the asset inventory
   b) Document asset treatment in the SSP
   c) Show these assets are managed using the contractor's risk-based security policies, procedures, and practices
   d) Document in the network diagram of the CMMC Assessment Scope
2) CMMC Assessment Requirements:
   a) Review the SSP
   b) Do not assess against other CMMC security requirements

Out of Scope Assets[8]

1) Description:
   a) Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets
   b) Assets that are physically or logically separated from CUI assets and do not provide security protections for CUI Assets are also Out-of-Scope Assets.
   c) Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset
   d) An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset
2) Your Requirement:
   a) Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI
3) CMMC Requirements:
   a) None

[5] Source: as defined in NIST SP 800-160v2 Rev 1 (incorporated by reference, see 32 CFR § 170.2.) NOTE: Operational Technology (OT) specifically includes Supervisory Control and Data Acquisition (SCADA); this is a rapidly evolving field. [Source: NIST SP 800-82r3]
[6] Federal Acquisition Regulation (FAR) 52.245-1
[7] OT includes hardware and software that use direct monitoring and control of industrial equipment to detect or cause a change.
[8] 32 CFR § 170.19(c)(1)

Additional Guidance on Level 2

Separation Techniques

Separation is a system architecture design concept that can provide physical/logical isolation of assets that process, transmit, or store CUI from assets not involved with CUI. Effective separation involves logically or physically separating assets and is required only for Out-of-Scope Assets. By separating assets, the CMMC Assessment Scope can be limited.[9]

1) Logical separation occurs when data transfer between physically connected assets (wired or wireless) is prevented by non-physical means such as software or network assets (e.g., firewall, routers, VPNs, VLANs).
2) Physical separation occurs when assets have no connection (wired or wireless). Data can only be transferred manually (e.g., USB drive).

When is a new assessment required:

A new assessment is required if there are significant architectural or boundary changes to the previous CMMC Assessment Scope. Examples include, but are not limited to, expansions of networks or mergers and acquisitions.

When your annual affirmation is acceptable:

Operational changes within a CMMC Assessment Scope, such as adding or subtracting resources within the existing assessment boundary that follow the existing SSP.

External Service Provider Considerations

An External Service Provider (ESP) can be within the OSA's scope of CMMC requirements if it meets CUI Asset and/or Security Protection Asset criteria. To be considered an ESP, data (specifically CUI or Security Protection Data, e.g., log data, configuration data) must reside on the ESP assets.[10]

1) The use of an ESP, its relationship to your company, and the services provided need to be documented in your SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of your company and ESP with respect to the services provided.
2) Evaluate the ESP's CRM where the provider identifies security requirement objectives that are the provider's responsibility and security requirement objectives that are your responsibility.
3) Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support your company's information security objectives.

[9] NIST SP 800-171 Rev 2,
[10] 32 CFR § 170.19(c)(2)

4) ESPs that are CSPs:
    a) and store, process, or transmit CUI, must meet the FedRAMP requirements in DFARS clause 252.204-7012.
    b) and do NOT store, process, or transmit CUI, are not required to meet FedRAMP requirements in DFARS clause 252.204-7012. Services provided by an ESP are in the your assessment scope.
5) ESPs that are not a CSP:
    a) and store, process, or transmit CUI, require assessment. The ESP services used to meet your company's CMMC requirements are within the scope of your CMMC assessment.
    b) and do NOT store, process, or transmit CUI, do not require their own CMMC assessment. Services provided by an ESP are in your assessment scope.
    c) may voluntarily request a C3PAO assessment, and a C3PAO may conduct such an assessment, if the ESP makes that business decision.
6) Your company shall also be assessed at Level 2, as applicable, against their on-premise infrastructure connecting to the CSP. As part of the CMMC Assessment Scope, the security requirements from the CRM must be documented or referred to in your SSP, which will also be assessed.
7) ESPs can be part of the same corporate/organizational structure but still be external to your company such as a centralized SOC or NOC which supports multiple business units. The same requirements apply and are based on whether or not the ESP provides cloud services and whether or not the ESP processes, stores, or transmits CUI on their systems.
8) An ESP that is used as staff augmentation and the OSA provides all processes, technology, and facilities does not need CMMC assessment.
9) When ESPs are assessed as part of your CMMC assessment, the type of the assessment is dictated by your company's DoD solicitation and contract requirement.

Cloud Service Provider (CSP)

Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. (e.g., networks, servers, storage, applications, and services). An ESP would be considered a CSP when it provides its own cloud services

An ESP (not a CSP) that provides technical support services to its clients would be considered a Managed Service Provider. It does not host its own cloud platform offering. An ESP may utilize cloud offerings to deliver services to clients without being a CSP.

An ESP that manages a third-party cloud service on behalf of an OSA would not be considered a CSP.

Not all companies that provide services to an OSA should be considered an ESP. Cloud based services such as human resource and accounting SaaS applications typically do not contribute to the security of the OSA's environment; process or store SPD; or process, store, or transmit CUI. The OSA must determine if the company providing the service should be considered an ESP based on the services provided and if CUI is processed, stored, or transmitted.

FCI and CUI

FCI and CUI in the Same Assessment Scope

1) A Level 2 self-assessment or Level 2 certification assessment satisfies the Level 1 self-assessment requirements for the same CMMC Assessment Scope. If FCI is processed, stored, or transmitted within the same scope as CUI in the Level 2 scope, then the methods to implement the Level 2 security requirements apply towards meeting the Level 1 assessment objectives. You are responsible for ensuring that only authorized users and processes have access to data regardless of its designation.

FCI and CUI in Different Assessment Scopes

1) If FCI and CUI do not share an environment, the two assessments would be conducted independently and methods to implement security requirements in one scope would not apply to the other scope.

Use of Enclaves

Satisfaction of CMMC security requirements may be accomplished by people, processes, or technologies which apply to your entire enterprise. This does not mean all assets across your entire enterprise are automatically part of a CMMC Assessment Scope.

a) For example, a centralized IT group may acquire, configure, deploy, and maintain a standard anti-malware tool. Systems within a defined assessment scope use that centrally deployed tool. The antimalware tool and the people in the IT group who maintain it, the processes and policies to deploy and update it, and the supporting systems (e.g., management server) could be in the CMMC Assessment Scope but other functions performed by the enterprise IT and other enterprise assets would not be automatically part of the CMMC Assessment Scope.

Within the enclave, your company determines which requirements are implemented and which requirements are inherited; all requirements must be MET. If a process, policy, tool, or technology within the enclave would invalidate an implementation at the Enterprise level, that requirement cannot be inherited and you must demonstrate that it is MET by implementation in some other way.

Assessment

Level 2 incorporates the security requirements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Level 2 addresses the protection of Controlled Unclassified Information (CUI).[11]

Level 2 self-assessment requirements.

1) A self-assessment is the term for the activity performed by an entity to evaluate its own CMMC Level, as applied to Level 1 and some Level 2.[12]
   a) The Organization Seeking Assessment (OSA) must complete and achieve a MET result for all security requirements in in NIST SP 800-171 R2. to achieve the CMMC Status of Level 2 (Self).
2) The OSA must conduct a self-assessment in accordance with the procedures
   a) The OSA must conduct a Level 2 self-assessment in accordance with NIST SP 800-171A Jun2018 and the CMMC Level 2 scoping requirements for the information systems within the CMMC Assessment Scope.
   b) The Level 2 self-assessment must be scored in accordance with the CMMC Scoring Methodology and,
   c) The OSA must upload the results into SPRS.
      i) If a POA&M exists, a POA&M closeout self-assessment must be performed by the OSA when all NOT MET requirements have been remediated.
      ii) The POA&M closeout self-assessment must be performed within 180-days of the Conditional CMMC Status Date.
3) A Level 2 certification assessment is the term for the activity performed by a Certified Third-Party Assessment Organization (C3PAO) to evaluate the CMMC level of your company.
   a) Level 2 certification assessment requires the OSA to achieve the CMMC Status of either Conditional Level 2 (C3PAO) or Final Level 2 (C3PAO)[13]

Level 2 self-assessment with the use of Cloud Service Provider

An OSA may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (Self) under the following circumstances:

1) The CSP product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or
2) The CSP product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those

[11] 32 CFR § 2002.4(h)
[12] 32 CFR § 170.4, 32 CFR § 170.15 to 32 CFR § 170.18
[13] 32 § CFR 170.4,

established by the FedRAMP Moderate (or higher) baseline. FedRAMP Moderate or FedRAMP Moderate equivalent is in accordance with DoD Policy.

3) The OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the Customer Responsibility Matrix (CRM) must be documented or referred to in the OSA's System Security Plan (SSP).[14]

Documents

For some security requirements, review of documentation may assist an entity in determining if the assessment objectives have been met. Interviews with staff may help identify relevant documents. Documents need to be in their final forms; drafts of policies or documentation are not eligible to be used as evidence because they are not yet official and still subject to change.[15] Common types of documents that may be used as evidence include:

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive.

Assessment Findings

The self-assessment of a CMMC requirement results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE[16]

1) To demonstrate Level 2 compliance, you will need a finding of MET or NOT APPLICABLE on all Level 2 security requirements.
2) MET: All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include working papers, drafts, and unofficial or unapproved policies. For each security requirement marked MET, it is best practice to record statements that indicate the response conforms to all objectives and document the appropriate evidence to support the response.
    a) Enduring Exceptions when described, along with any mitigations, in the system security plan shall be assessed as MET.

[14] 32 CFR § 170.19(c)(2)
[15] 32 CFR § 170.24,
[16] 32 CFR § 170.24.

b) Temporary deficiencies that are appropriately addressed in operational plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) shall be assessed as MET.

3) NOT MET: One or more objectives of the security requirement is not satisfied. For each security requirement marked NOT MET, it is best practice to record statements that explain why and document the appropriate evidence showing that does not conform fully to all of the objectives. One NOT MET Assessment Objective results in a failure of the entire security requirement. A security requirement can be applicable even when assessment objectives included in the security requirement are scored N/A. The security requirement is NOT MET when one or more applicable assessment objectives is NOT MET.
4) NOT APPLICABLE (N/A): A security requirement and/or objective do not apply at the time of the assessment. For each security requirement marked N/A, it is best practice to record a statement that explains why the requirement does not apply. During an assessment, an assessment objective assessed as N/A is equivalent to the same assessment objective being assessed as MET. Each assessment objective in NIST SP 800-171A must yield a finding of MET or NOT APPLICABLE in order for the overall security requirement to be scored as MET.

   For example, SC.L1-b.1.xi might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope.

Satisfaction of security requirements may be accomplished by other parts of the enterprise or an External Service Provider (ESP)[17]. A security requirement is considered MET if adequate evidence is provided that the enterprise or ESP implements the requirement objectives. An ESP may be external people, technology, or facilities that is used, including cloud service providers, managed service providers, managed security service providers, or cybersecurity-as-a-service providers.

[17] 32 CFR § 170.4

Assessment Items [18]

Access Control

AC.L2-3.1.1– Authorized Access Control [CUI Data]

Identify users, processes, and devices that are allowed to use company computers and can log on to the company network.[19]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

Example 1

Your company maintains a list of all personnel authorized to use company information systems [a]. This list is used to support identification and authentication activities conducted by IT when authorizing access to systems [a,d].

Example 2

A coworker wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will prevent network access by unauthorized systems and devices [c]. You help the coworker submit a ticket that asks for the printer to be granted access to the network, and appropriate leadership approves the device [f].

AC.L2-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Determine if:

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[18] NIST SP 800-171A
[19] NIST SP 800-171 Rev. 2 3.1.1 • FAR Clause 52.204-21 b.1.i

[b] system access is limited to the defined types of transactions and functions for authorized users.

Example

Your team manages DoD contracts for your company. Members of your team need to access the contract information to perform their work properly. Because some of that data contains CUI, you work with IT to set up your group's systems so that users can be assigned access based on their specific roles [a]. Each role limits whether an employee has read-access or create/read/delete/update -access [b]. Implementing this access control restricts access to CUI information unless specifically authorized. [20]

AC.L2-3.1.3 – CONTROL CUI FLOW

Control the flow of CUI in accordance with approved authorizations.

Determine if:

[a] information flow control policies are defined;

[b] methods and enforcement mechanisms for controlling the flow of CUI are defined;

[c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified;

[d] authorizations for controlling the flow of CUI are defined; and

[e] approved authorizations for controlling the flow of CUI are enforced. [21]

Example

You configure a proxy device on your company's network. CUI is stored within this environment. Your goal is to better mask and protect the devices inside the network while enforcing information flow policies. After the device is configured, information does not flow directly from the internal network to the internet. The proxy device intercepts the traffic and analyzes it to determine if the traffic conforms to organization information flow control policies. If it does, the device allows the information to pass to its destination [b]. The proxy blocks traffic that does not meet policy requirements [e].

Example 2

As a subcontractor on a DoD contract, your organization sometimes needs to transmit CUI to the prime contractor. You create a policy document that specifies who is allowed to transmit CUI and that such transmission requires manager approval [a,c,d]. The policy instructs users to encrypt any CUI transmitted via email or to use a designated secure file sharing utility [b,d].

[20] NIST SP 800-171 Rev. 2 3.1.2 • FAR Clause 52.204-21 b.1.ii
[21] NIST SP 800-171 Rev. 2 3.1.3

The policy states that users who do not follow appropriate procedures may be subject to disciplinary action [e].

AC.L2-3.1.4 – SEPARATION OF DUTIES

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Determine if:

[a] the duties of individuals requiring separation are defined;

[b] responsibilities for duties that require separation are assigned to separate individuals; and

[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.[22]

Example 1

You are responsible for the management of several key systems within your organization including some that process CUI. You assign the task of reviewing the system logs to two different people. This way, no one person is solely responsible for the execution of this critical security function [c].

Example 2

You are a system administrator. Human Resources notifies you of a new hire, and you create an account with general privileges, but you are not allowed to grant access to systems that contain CUI [a,b]. The program manager contacts the team in your organization that has system administration authority over the CUI systems and informs them which CUI the new hire will need to access. Subsequently, a second system administrator grants access privileges to the new hire [c].[23]

AC.L2-3.1.5 – LEAST PRIVILEGE

Employ the principle of least privilege, including for specific security functions and privileged accounts.

Determine if:

[a] privileged accounts are identified;

[b] access to privileged accounts is authorized in accordance with the principle of least privilege; [c] security functions are identified; and

[d] access to security functions is authorized in accordance with the principle of least privilege.

---

[22] NIST SP 800-171A, p. 10
[23] NIST SP 800-171 Rev. 2, p. 11.

Example You create accounts for an organization that processes CUI. By default, everyone is assigned a basic user role, which prevents a user from modifying system configurations. Privileged access is only assigned to users and processes that require it to carry out job functions, such as IT staff, and is very selectively granted [b,d].[24]

AC.L2-3.1.6 – NON-PRIVILEGED ACCOUNT USE

Use non-privileged accounts or roles when accessing nonsecurity functions.

Determine if:

[a] nonsecurity functions are identified; and

[b] users are required to use non-privileged accounts or roles when accessing nonsecurity functions.[25]

Example

You are logged in using your privileged account and you need to look up how to reset a nonfunctioning application which processes CUI. You should log on to another computer with your non-privileged account before you connect to the web and start searching for the reset information [b]. That way, if your account is compromised during the search, it will be your regular user account rather than an account with elevated privileges.

AC.L2-3.1.7 – PRIVILEGED FUNCTIONS

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Determine if:

[a] privileged functions are defined;

[b] non-privileged users are defined;

[c] non-privileged users are prevented from executing privileged functions; and

[d] the execution of privileged functions is captured in audit logs.

Example

Your organization handles CUI and has put security controls in place that prevent nonprivileged users from performing privileged activities [a,b,c]. However, a standard user was accidentally given elevated system administrator privileges. The organization has implemented an endpoint detection and response solution that provides visibility into the use of privileged activities. The monitoring system logs a security misconfiguration because the use of

[24] NIST SP 800-171 Rev. 2, p. 12.
[25] NIST SP 800-171A, p. 11.

administrative privileges was performed by a user who was not known to have that ability. This allows you to correct the error [d].

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

Limit unsuccessful logon attempts.

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Example

You attempt to log on to your work computer, which stores CUI. You mistype your password three times in a row, and an error message is generated telling you the account is locked [b]. You call your IT help desk or system administrator to request assistance. The system administrator explains that the account is locked as a result of three unsuccessful logon attempts [a]. The administrator offers to unlock the account and notes that you can wait 30 minutes for the account to unlock automatically.

AC.L2-3.1.9 – PRIVACY & SECURITY NOTICES

Provide privacy and security notices consistent with applicable CUI rules.

Determine if:

[a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category; and

[b] privacy and security notices are displayed.

Example

You are setting up IT equipment including a database server that will contain CUI. You have worked with legal counsel to draft a notification. It contains both general and specific CUI security and privacy requirements [a]. The system displays the required security and privacy information before anyone logs on to your organization's computers that contain or provide access to CUI [b].

AC.L2-3.1.10 – SESSION LOCK

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Determine if:

[a] the period of inactivity after which the system initiates a session lock is defined;

[b] access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; and

[c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.

Example

You manage systems for an organization that stores, processes, and transmits CUI. You notice that employees leave their offices without locking their computers. Sometimes their screens display sensitive company information. You configure all machines to lock after five minutes of inactivity [a,b]. You also remind your coworkers to lock their systems when they walk away [a].

AC.L2-3.1.11 – SESSION TERMINATION

Terminate (automatically) a user session after a defined condition.

Determine if:

[a] conditions requiring a user session to terminate are defined; and

[b] a user session is automatically terminated after any of the defined conditions occur.

Example 1

You manage systems containing CUI for your organization and configure the system to terminate all user sessions after 1 hour of inactivity [a]. As the session timeout approaches, the system prompts users with a warning banner asking if they want to continue the session. When the session timeout does occur, the login page pops up, and the users must log in to start a new session [b].

Example 2

A user is logged into a corporate database containing CUI but is not authorized to view CUI. The user has submitted a series of queries that unintentionally violate policy, as they attempt to extract CUI that the user is not authorized to view [a]. The session terminates with a warning as a result of a violation of corporate policy [b]. The user must reestablish the session before being able to submit additional legitimate queries.

AC.L2-3.1.12 – CONTROL REMOTE ACCESS

Monitor and control remote access sessions.

Determine if:

[a] remote access sessions are permitted;

[b] the types of permitted remote access are identified;

[c] remote access sessions are controlled; and

[d] remote access sessions are monitored.

Example

You often need to work from remote locations, such as your home or client sites, and you are permitted to access your organization's internal networks (including a network containing CUI) from those remote locations [a]. A system administrator issues you a company laptop with VPN software installed, which is required to connect to the networks remotely [b]. After the laptop connects to the VPN server, you must accept a privacy notice that states that the company's security department may monitor the connection. This monitoring is achieved through the analysis of data from sensors on the network notifying IT if issues arise. The security department may also review audit logs to see who is connecting remotely, when, and what information they are accessing [d]. During session establishment, the message "Verifying Compliance" means software like a Device Health Check (DHC) application is checking the remote device to ensure it meets the established requirements to connect [c].

AC.L2-3.1.13 – REMOTE ACCESS CONFIDENTIALITY

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Determine if:

[a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and

[b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.

Example

You are responsible for implementing a remote network access capability for users who access CUI remotely. In order to provide session confidentiality, you decide to implement a VPN mechanism and select a product that has completed FIPS 140 validation [a,b].

AC.L2-3.1.14 – REMOTE ACCESS ROUTING

Route remote access via managed access control points.

Determine if:

[a] managed access control points are identified and implemented; and

[b] remote access is routed through managed network access control points.

Example

You manage systems for a company that processes CUI at multiple locations, and several employees at different locations need to connect to the organization's networks while working remotely. Because each company location has a direct connection to headquarters, you

decide to route all remote access through the headquarters location [a]. All remote traffic is routed through a single location to simplify monitoring [b].

AC.L2-3.1.15 – PRIVILEGED REMOTE ACCESS

Authorize remote execution of privileged commands and remote access to security-relevant information.

Determine if:

[a] privileged commands authorized for remote execution are identified;

[b] security-relevant information authorized to be accessed remotely is identified;

[c] the execution of the identified privileged commands via remote access is authorized; and

[d] access to the identified security-relevant information via remote access is authorized.

Example

Your company's Access Control Policy permits certain work roles to remotely perform a limited set of privileged commands from company-owned computers [a]. You implement controls to enforce who can remotely execute a privileged command, which privileged commands they can execute, and who is allowed access to security relevant information such as audit log configuration settings [a,c,d].

AC.L2-3.1.16 – WIRELESS ACCESS AUTHORIZATION

Authorize wireless access prior to allowing such connections.

Determine if:

[a] wireless access points are identified; and

[b] wireless access is authorized prior to allowing such connections.

Example

Your company is implementing a wireless network at its headquarters. CUI may be transmitted on this network. You work with management to draft a policy about the use of the wireless network. The policy states that only company-approved devices that contain verified security configuration settings are allowed to connect. The policy also includes usage restrictions that must be followed for anyone who wants to use the wireless network. Authorization is required before devices are allowed to connect to the wireless network [b].

AC.L2-3.1.17 – WIRELESS ACCESS PROTECTION

Protect wireless access using authentication and encryption.

Determine if:

[a] wireless access to the system is protected using authentication; and

[b] wireless access to the system is protected using encryption.

Example 1

You manage the wireless network at a small company and are installing a new wireless solution that may transmit CUI. You start by selecting a product that employs encryption validated against the FIPS 140 standard. You configure the wireless solution to use WPA2, requiring users to enter a pre-shared key to connect to the wireless network [a,b].

Example 2

You manage the wireless network at a large company and are installing a new wireless solution that may transmit CUI. You start by selecting a product that employs encryption that is validated against the FIPS 140 standard. Because of the size of your workforce, you configure the wireless system to authenticate users with a RADIUS server. Users must provide the wireless system with their domain usernames and passwords to be able to connect, and the RADIUS server verifies those credentials. Users unable to authenticate are denied access [a,b].

AC.L2-3.1.18 – MOBILE DEVICE CONNECTION

Control connection of mobile devices.

Determine if:

[a] mobile devices that process, store, or transmit CUI are identified;

[b] mobile device connections are authorized; and

[c] mobile device connections are monitored and logged

Example

Your organization has a policy stating that all mobile devices, including iPads, tablets, mobile phones, and Personal Digital Assistants (PDAs), must be approved and registered with the IT department before connecting to the network that contains CUI. The IT department uses a Mobile Device Management solution to monitor mobile devices and enforce policies across the enterprise [b,c].

AC.L2-3.1.19 – ENCRYPT CUI ON MOBILE

Encrypt CUI on mobile devices and mobile computing platforms.

Determine if:

[a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; and

[b] encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.

Example

You are in charge of mobile device security for a company that processes CUI. You configure all laptops to use the full-disk encryption technology built into the operating system. This approach is FIPS-validated and encrypts all files, folders, and volumes. Phones and tablets pose a greater technical challenge with their wide range of manufacturers and operating systems. You select a proprietary mobile device management (MDM) solution to enforce FIPS-validated encryption on those devices [a,b].

AC.L2-3.1.20 – EXTERNAL CONNECTIONS [CUI DATA]

Verify and control/limit connections to and use of external systems.

Determine if:

[a] connections to external systems are identified;

[b] the use of external systems is identified;

[c] connections to external systems are verified;

[d] the use of external systems is verified;

[e] connections to external systems are controlled/limited; and

[f] the use of external systems is controlled/limited.

Example

Your company has a project that contains CUI. You remind your coworkers of the policy requirement to use their company laptops, not personal laptops or tablets, when working remotely on the project [b,f]. You also remind everyone to work from the cloud environment that is approved for processing and storing CUI rather than the other collaborative tools that may be used for other projects [b,f].

AC.L2-3.1.21 – PORTABLE STORAGE USE

Limit use of portable storage devices on external systems.

Determine if:

[a] the use of portable storage devices containing CUI on external systems is identified and documented;

[b] limits on the use of portable storage devices containing CUI on external systems are defined; and

[c] the use of portable storage devices containing CUI on external systems is limited as defined.

Example

Your organization, which stores and processes CUI, has a written portable device usage restriction policy. It states that users can only use external storage devices such as thumb dives or external hard disks that belong to the company. When needed for a specific business function, a user checks the device out from IT and returns it to IT when no longer needed [a,b].

AC.L2-3.1.22 – CONTROL PUBLIC INFORMATION [CUI DATA]

Control CUI posted or processed on publicly accessible systems.

Determine if:

[a] individuals authorized to post or process information on publicly accessible systems are identified;

[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified;

[c] a review process is in place prior to posting of any content to publicly accessible systems;

[d] content on publicly accessible systems is reviewed to ensure that it does not include CUI; and

[e] mechanisms are in place to remove and address improper posting of CUI.

Example

Your company decides to start issuing press releases about its projects in an effort to reach more potential customers. Your company receives CUI from the government as part of its DoD contract. Because you recognize the need to manage controlled information, including CUI, you meet with the employees who write the releases and post information to establish a review process [c]. It is decided that you will review press releases for CUI before posting it on the company website [a,d]. Only certain employees will be authorized to post to the website [a].

Awareness and Training

AT.L2-3.2.1 – ROLE-BASED RISK AWARENESS

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Determine if:

[a] security risks associated with organizational activities involving CUI are identified;

[b] policies, standards, and procedures related to the security of the system are identified;

[c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities; and

[d] managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

Example

Your organization holds a DoD contract which requires the use of CUI. You want to provide information to employees so they can identify phishing emails. To do this, you prepare a presentation that highlights basic traits, including:

1) suspicious-looking email address or domain name;
2) a message that contains an attachment or URL; and
3) a message that is poorly written and often contains obvious misspelled words. You encourage everyone to not click on attachments or links in a suspicious email [c].

You tell employees to forward such a message immediately to IT security [d]. You download free security awareness posters to hang in the office [c,d]. You send regular emails and tips to all employees to ensure your message is not forgotten over time [c,d].

AT.L2-3.2.2 – ROLE-BASED TRAINING

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Determine if:

[a] information security-related duties, roles, and responsibilities are defined;

[b] information security-related duties, roles, and responsibilities are assigned to designated personnel; and

[c] personnel are adequately trained to carry out their assigned information security related duties, roles, and responsibilities.

Example

Your company upgraded the firewall to a newer, more advanced system to protect the CUI it stores. You have been identified as an employee who needs training on the new device [a,b,c]. This will enable you to use the firewall effectively and efficiently. Your company considered training resources when it planned for the upgrade and ensured that training funds were available as part of the upgrade project [c].

AT.L2-3.2.3 – INSIDER THREAT AWARENESS

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Determine if:

[a] potential indicators associated with insider threats are identified; and

[b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

Example

You are responsible for training all employees on the awareness of high-risk behaviors that can indicate a potential insider threat [b]. You educate yourself on the latest research on insider threat indicators by reviewing a number of law enforcement bulletins [a]. You then add the following example to the training package: A baseline of normal behavior for work schedules has been created. One employee's normal work schedule is 8:00 AM–5:00 PM, but another employee noticed that the employee has been working until 9:00 PM every day even though no projects requiring additional hours have been assigned [b]. The observing employee reports the abnormal work schedule using the established reporting guidelines.

Audit and Accountability

AU.L2-3.3.1 – SYSTEM AUDITING

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

Determine if:

[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified;

[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined;

[c] audit records are created (generated);

[d] audit records, once created, contain the defined content;

[e] retention requirements for audit records are defined; and

[f] audit records are retained as defined.

Example

You set up audit logging capability for your company. You determine that all systems that contain CUI must have extra detail in the audit logs. Because of this, you configure these systems to log the following information for all user actions [b,c]:

a) time stamps;
b) source and destination addresses;
c) user or process identifiers;
d) event descriptions;
e) success or fail indications; and
f) filenames.

AU.L2-3.3.2 – USER ACCOUNTABILITY

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Determine if:

[a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and

[b] audit records, once created, contain the defined content.

Example

You manage systems for a company that stores, processes, and transmits CUI. You want to ensure that you can trace all remote access sessions to a specific user. You configure the VPN device to capture the following information for all remote access connections: source and destination IP address, user ID, machine name, time stamp, and user actions during the remote session [b].

AU.L2-3.3.3 – EVENT REVIEW

Review and update logged events.

Determine if:

[a] a process for determining when to review logged events is defined;

[b] event types being logged are reviewed in accordance with the defined review process; and

[c] event types being logged are updated based on the review.

Example

You are in charge of IT operations for a company that processes CUI and are responsible for identifying and documenting which events are relevant to the security of your company's systems. Your company has decided that this list of events should be updated annually or when new security threats or events have been identified, which may require additional events to be logged and reviewed [a]. The list of events you are capturing in your logs started as the list of recommended events given by the manufacturers of your operating systems and devices, but it has grown from experience.

Your company experiences a security incident, and a forensics review shows the logs appear to have been deleted by a remote user. You notice that remote sessions are not currently being logged [b]. You update the list of events to include logging all VPN sessions [c].

AU.L2-3.3.4 – AUDIT FAILURE ALERTING

Alert in the event of an audit logging process failure.

Determine if:

[a] personnel or roles to be alerted in the event of an audit logging process failure are identified;

[b] types of audit logging process failures for which alert will be generated are defined; and

[c] identified personnel or roles are alerted in the event of an audit logging process failure.

Example

You are in charge of IT operations for a company that processes CUI, and your responsibilities include managing the audit logging process. You configure your systems to send you an email in the event of an audit log failure. One day, you receive one of these alerts. You connect to the system, restart logging, and determine why the logging stopped [a,b,c].

AU.L2-3.3.5 – AUDIT CORRELATION

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Determine if:

[a] audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined; and

[b] defined audit record review, analysis, and reporting processes are correlated.

Example

You are a member of a cyber defense team responsible for audit log analysis. You run an automated tool that analyzes all the audit logs across a Local Area Network (LAN) segment simultaneously looking for similar anomalies on separate systems at separate locations. Some of these systems store CUI. After extracting anomalous information and performing a correlation analysis [b], you determine that four different systems have had their event log information cleared between 2:00 AM to 3:00 AM, although the associated dates are different. The team monitors all systems on the same LAN segment between 2:00 AM to 3:00 AM for the next 30 days.

AU.L2-3.3.6 – REDUCTION & REPORTING

Provide audit record reduction and report generation to support on-demand analysis and reporting.

Determine if:

[a] an audit record reduction capability that supports on-demand analysis is provided; and

[b] a report generation capability that supports on-demand reporting is provided.

Example

You are in charge of IT operations in a company that processes CUI. You are responsible for providing audit record reduction and report generation capability. To support this function, you deploy an open-source solution that will collect and analyze data for signs of anomalies. The solution queries your central log repository to extract relevant data and provide you with a concise and comprehensive view for further analysis to identify potentially malicious activity [a]. In addition to creating on-demand data sets for analysis, you create customized reports explaining the contents of the data set [b].

AU.L2-3.3.7 – AUTHORITATIVE TIME SOURCE

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Determine if:

[a] internal system clocks are used to generate time stamps for audit records;

[b] an authoritative source with which to compare and synchronize internal system clocks is specified; and

[c] internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.

Example

You are setting up several new computers on your company's network, which contains CUI. You update the time settings on each machine to use the same authoritative time server on the internet [b,c]. When you review audit logs, all your machines will have synchronized time, which aids in any potential security investigations.

AU.L2-3.3.8 – AUDIT PROTECTION

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Determine if:

[a] audit information is protected from unauthorized access;

[b] audit information is protected from unauthorized modification;

[c] audit information is protected from unauthorized deletion;

[d] audit logging tools are protected from unauthorized access;

[e] audit logging tools are protected from unauthorized modification; and

[f] audit logging tools are protected from unauthorized deletion.

Example

You are in charge of IT operations in a company that handles CUI. Your responsibilities include protecting audit information and audit logging tools. You protect the information from modification or deletion by having audit log events forwarded to a central server and by restricting the local audit logs to only be viewable by the system administrators [a,b,c]. Only a small group of security professionals can view the data on the central audit server [b,c,d]. For an additional layer of protection, you back up the server daily and encrypt the backups before sending them to a cloud data repository [a,b,c].

AU.L2-3.3.9 – AUDIT MANAGEMENT

Limit management of audit logging functionality to a subset of privileged users.

Determine if:

[a] a subset of privileged users granted access to manage audit logging functionality is defined; and

[b] management of audit logging functionality is limited to the defined subset of privileged users.

Example

You are responsible for the administration of select company infrastructure that contains CUI, but you are not responsible for managing audit information. You are not permitted to review

audit logs, delete audit logs, or modify audit log settings [b]. Full control of audit logging functions has been given to senior system administrators [a,b]. This separation of system administration duties from audit logging management is necessary to prevent possible log file tampering.

Configuration Management

CM.L2-3.4.1 – SYSTEM BASELINING

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Determine if:
[a] a baseline configuration is established;
[b] the baseline configuration includes hardware, software, firmware, and documentation;
[c] the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle;
[d] a system inventory is established;
[e] the system inventory includes hardware, software, firmware, and documentation; and
[f] the inventory is maintained (reviewed and updated) throughout the system development life cycle
Example
You are in charge of upgrading the computer operating systems of your office's computers. Some of these computers process, store, or transmit CUI. You research how to set up and configure a workstation with the least functionality and highest security and use that as the framework for creating a configuration that minimizes functionality while still allowing users to do their tasks. After testing the new baseline on a single workstation, you document this configuration and apply it to the other computers [a]. You then check to make sure that the software changes are accurately reflected in your master system inventory [e]. Finally, you set a calendar reminder to review the baseline in three months [f].

CM.L2-3.4.2 – SECURITY CONFIGURATION ENFORCEMENT

Establish and enforce security configuration settings for information technology products employed in organizational systems.

Determine if:

[a] security configuration settings for information technology products employed in the system are established and included in the baseline configuration; and

[b] security configuration settings for information technology products employed in the system are enforced.

Example

You manage baseline configurations for your company's systems, including those that process, store, and transmit CUI. As part of this, you download a secure configuration guide for each of your asset types (servers, workstations, network components, operating systems, middleware, and applications) from a well-known and trusted IT security organization. You then apply all of the settings that you can while still ensuring the assets can perform the role for which they are needed. Once you have the configuration settings identified and tested, you document them to ensure all applicable machines can be configured the same way [a,b].

CM.L2-3.4.3 – SYSTEM CHANGE MANAGEMENT

Track, review, approve or disapprove, and log changes to organizational systems.

Determine if:

[a] changes to the system are tracked;

[b] changes to the system are reviewed;

[c] changes to the system are approved or disapproved; and

[d] changes to the system are logged.

Example

Once a month, the management and technical team leads join a change control board meeting. During this meeting, everyone reviews all proposed changes to the environment [b,c]. This includes changes to the physical and computing environments. The meeting ensures that relevant subject-matter experts review changes and propose alternatives where needed.

CM.L2-3.4.4 – SECURITY IMPACT ANALYSIS

Analyze the security impact of changes prior to implementation.

Determine if:

[a] the security impact of changes to the system is analyzed prior to implementation.

Example

You have been asked to deploy a new web browser plug-in. Your standard change management process requires that you produce a detailed plan for the change, including a review of its potential security impact. A subject-matter expert who did not submit the change

reviews the plan and tests the new plug-in for functionality and security. You update the change plan based on the expert's findings and submit it to the change control board for final approval [a].

CM.L2-3.4.5 – ACCESS RESTRICTIONS FOR CHANGE

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Determine if:

[a] physical access restrictions associated with changes to the system are defined;

[b] physical access restrictions associated with changes to the system are documented;

[c] physical access restrictions associated with changes to the system are approved;

[d] physical access restrictions associated with changes to the system are enforced;

[e] logical access restrictions associated with changes to the system are defined;

[f] logical access restrictions associated with changes to the system are documented;

[g] logical access restrictions associated with changes to the system are approved; and

[h] logical access restrictions associated with changes to the system are enforced.

Example Your datacenter requires expanded storage capacity in a server. The change has been approved, and security is planning to allow an external technician to access the building at a specific date and time under the supervision of a manager [a,b,c,d]. A system administrator creates a temporary privileged account that can be used to log into the server's operating system and update storage settings [e,f,g]. On the appointed day, the technician is escorted into the datacenter, upgrades the hardware, expands the storage in the operating system (OS), and departs. The manager verifies the upgrade and disables the privileged account [h].

CM.L2-3.4.6 – LEAST FUNCTIONALITY

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Determine if:

[a] essential system capabilities are defined based on the principle of least functionality; and

[b] the system is configured to provide only the defined essential capabilities.

Example

You have ordered a new server, which has arrived with a number of free utilities installed in addition to the operating system. Before you deploy the server, you research the utilities to determine which ones can be eliminated without impacting functionality. You remove the unneeded software, then move on to disable unused ports and services. The server that enters production therefore has only the essential capabilities enabled for the system to function in its role [a,b].

CM.L2-3.4.7 – NONESSENTIAL FUNCTIONALITY

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Determine if:

[a] essential programs are defined;

[b] the use of nonessential programs is defined;

[c] the use of nonessential programs is restricted, disabled, or prevented as defined;

[d] essential functions are defined;

[e] the use of nonessential functions is defined;

[f] the use of nonessential functions is restricted, disabled, or prevented as defined;

[g] essential ports are defined;

[h] the use of nonessential ports is defined;

[i] the use of nonessential ports is restricted, disabled, or prevented as defined;

[j] essential protocols are defined;

[k] the use of nonessential protocols is defined;

[l] the use of nonessential protocols is restricted, disabled, or prevented as defined;

[m] essential services are defined;

[n] the use of nonessential services is defined; and

[o] the use of nonessential services is restricted, disabled, or prevented as defined.

Example

You are responsible for purchasing new endpoint hardware, installing organizationally required software to the hardware, and configuring the endpoint in accordance with the organization's policy. The organization has a system imaging capability that loads all necessary software, but it does not remove unnecessary services, eliminate the use of certain protocols, or close

unused ports. After imaging the systems, you close all ports and block the use of all protocols except the following:

• TCP for SSH on port 22;

• SMTP on port 25;

• TCP and UDP on port 53; and

• HTTP and HTTPS on port 443.

The use of any other ports or protocols are allowed by exception only [i,l,o].

CM.L2-3.4.8 – APPLICATION EXECUTION POLICY

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Determine if:

[a] a policy specifying whether whitelisting or blacklisting is to be implemented is specified;

[b] the software allowed to execute under whitelisting or denied use under blacklisting is specified; and

[c] whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.

Example To improve your company's protection from malware, you have decided to allow only designated programs to run. With additional research you identify a capability within the latest operating system that can control executables, scripts, libraries, or application installers run in your environment [c]. To ensure success you begin by authorizing digitally signed executables. Once they are deployed, you then plan to evaluate and deploy whitelisting for software libraries and scripts [c].

CM.L2-3.4.9 – USER-INSTALLED SOFTWARE

Control and monitor user-installed software.

Determine if:

[a] a policy for controlling the installation of software by users is established;

[b] installation of software by users is controlled based on the established policy; and

[c] installation of software by users is monitored.

Example

You are a system administrator. A user calls you for help installing a software package. They are receiving a message asking for a password because they do not have permission to install the software. You explain that the policy prohibits users from installing software without approval [a]. When you set up workstations for users, you do not provide administrative privileges. After the call, you redistribute the policy to all users ensuring everyone in the company is aware of the restrictions.

Identification and Authentication (IA)

IA.L2-3.5.1 – IDENTIFICATION [CUI DATA]

Identify system users, processes acting on behalf of users, and devices.

Determine if:

[a] system users are identified;

[b] processes acting on behalf of users are identified; and

[c] devices accessing the system are identified.

Example You want to make sure that all employees working on a project can access important information about it. Because this is work for the DoD and may contain CUI, you also need to prevent employees who are not working on that project from being able to access the information. You assign each employee is assigned a unique user ID, which they use to log into the system [a].

IA.L2-3.5.2 – AUTHENTICATION [CUI DATA]

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Determine if:

[a] the identity of each user is authenticated or verified as a prerequisite to system access;

[b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and

[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.[26]

Example 1

You are in charge of purchasing. You know that some laptops come with a default username and password. You notify IT that all default passwords should be reset prior to laptop use [a]. You ask IT to explain the importance of resetting default passwords and convey how easily they are discovered using internet searches during next week's cybersecurity awareness training.

Example 2

Your company decides to use cloud services for email and other capabilities. Upon reviewing this requirement, you realize every user or device that connects to the cloud service must be authenticated. As a result, you work with your cloud service provider to ensure that only properly authenticated users and devices are allowed to connect to the system [a,c].

IA.L2-3.5.3 – MULTIFACTOR AUTHENTICATION

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Determine if:

[a] privileged accounts are identified;

[b] multifactor authentication is implemented for local access to privileged accounts;

[c] multifactor authentication is implemented for network access to privileged accounts; and

[d] multifactor authentication is implemented for network access to non-privileged accounts.

Example

You decide to implement multifactor authentication (MFA) to improve security of your network. Your first step is enabling MFA on VPN access to your internal network [c,d]. When users initiate remote access, they will be prompted for the additional authentication factor. Because you also use a cloud-based email solution, you require MFA for access to that resource as well [c,d]. Finally, you enable MFA for both local and network logins for the system administrator accounts used to patch and manage servers [a,b,c].

IA.L2-3.5.4 – REPLAY-RESISTANT AUTHENTICATION

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Determine if:

[a] replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.

Example

To protect your IT infrastructure, you understand that the methods for authentication must not be easily copied and re-sent to your systems by an adversary. You select Kerberos for authentication because of its built-in resistance to replay attacks. As a next step you upgrade all of your web applications to require Transport Layer Security (TLS), which also is replay resistant. Your use of MFA to protect remote access also confers some replay resistance.

IA.L2-3.5.5 – IDENTIFIER REUSE

Prevent reuse of identifiers for a defined period.

Determine if:

[a] a period within which identifiers cannot be reused is defined; and

[b] reuse of identifiers is prevented within the defined period.

Example

As a system administrator, you maintain a central directory/domain that holds the accounts for users, computers, and network devices. As part of your job, you issue unique usernames (e.g., riley@acme.com) for the staff to access resources. When you issue staff computers you also rename the computer to reflect to whom it is assigned (e.g., riley-laptop01). Riley has recently left the organization, so you must manage the former staff member's account. Incidentally, their replacement is also named Riley. In the directory, you do not assign the previous account to the new user, as policy has defined an identifier reuse period of 24 months [a]. In accordance with policy, you create an account called riley02 [b]. This account is assigned the appropriate permissions for the new user. A new laptop is also provided with the identifier of riley02-laptop01.

IA.L2-3.5.6 – IDENTIFIER HANDLING

Disable identifiers after a defined period of inactivity.

Determine if:

[a] a period of inactivity after which an identifier is disabled is defined; and

[b] identifiers are disabled after the defined period of inactivity.

Example

One of your responsibilities is to enforce your company's inactive account policy: any account that has not been used in the last 45 days must be disabled [a]. You enforce this by writing a script that runs once a day to check the last login date for each account and generates a report

of the accounts with no login records for the last 45 days. After reviewing the report, you notify each inactive employee's supervisor and disable the account [b].

IA.L2-3.5.7 – PASSWORD COMPLEXITY

Enforce a minimum password complexity and change of characters when new passwords are created.

Determine if:

[a] password complexity requirements are defined;

[b] password change of character requirements are defined;

[c] minimum password complexity requirements as defined are enforced when new passwords are created; and

[d] minimum password change of character requirements as defined are enforced when new passwords are created.

Example

You work with management to define password complexity rules and ensure they are listed in the company's security policy. You define and enforce a minimum number of characters for each password and ensure that a certain number of characters must be changed when updating passwords [a,b]. Characters include numbers, lowercase and uppercase letters, and symbols [a]. These rules help create hard-to-guess passwords, which help to secure your network.

IA.L2-3.5.8 – PASSWORD REUSE

Prohibit password reuse for a specified number of generations.

Determine if:

[a] the number of generations during which a password cannot be reused is specified and

[b] reuse of passwords is prohibited during the specified number of generations.

Example

You explain in your company's security policy that changing passwords regularly provides increased security by reducing the ability of adversaries to exploit stolen or purchased passwords over an extended period. You define how often individuals can reuse their passwords and the minimum number of password generations before reuse [a]. If a user tries

to reuse a password before the number of password generations has been exceeded, an error message is generated, and the user is required to enter a new password [b].

IA.L2-3.5.9 – TEMPORARY PASSWORDS

Allow temporary password use for system logons with an immediate change to a permanent password.

Determine if:

[a] an immediate change to a permanent password is required when a temporary password is used for system logon.

Example

One of your duties as a systems administrator is to create accounts for new users. You configure all systems with user accounts to require users to change a temporary password upon initial login to a permanent password [a]. When a user logs on for the first time, they are prompted to create a unique password that meets all of the defined complexity rules.

IA.L2-3.5.10 – CRYPTOGRAPHICALLY-PROTECTED PASSWORDS

Store and transmit only cryptographically-protected passwords.

Determine if:

[a] passwords are cryptographically protected in storage; and

[b] passwords are cryptographically protected in transit.

Example

You are responsible for managing passwords for your organization. You protect all passwords with a one-way transformation, or hashing, before storing them. Passwords are never transmitted across a network unencrypted [a,b].

IA.L2-3.5.11 – OBSCURE FEEDBACK

Obscure feedback of authentication information.

Determine if:

[a] authentication information is obscured during the authentication process.

Example

As a system administrator, you configure your systems to display an asterisk when users enter their passwords into a computer system [a]. For mobile devices, the password characters are

briefly displayed to the user before being obscured. This prevents people from figuring out passwords by looking over someone's shoulder.

Incident Response (IR)

IR.L2-3.6.1 – INCIDENT HANDLING

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Determine if:

[a] an operational incident-handling capability is established;

[b] the operational incident-handling capability includes preparation;

[c] the operational incident-handling capability includes detection;

[d] the operational incident-handling capability includes analysis;

[e] the operational incident-handling capability includes containment;

[f] the operational incident-handling capability includes recovery; and

[g] the operational incident-handling capability includes user response activities.

Example

Your manager asks you to set up your company's incident-response capability [a]. First, you create an email address to collect information on possible incidents. Next, you draft a contact list of all the people who need to know when an incident occurs. You document a procedure for how to submit incidents that includes roles and responsibilities when a potential incident is detected or reported. The procedure also explains how to track incidents, from initial creation to closure [b].

IR.L2-3.6.2 – INCIDENT REPORTING

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Determine if:

[a] incidents are tracked;

[b] incidents are documented;

[c] authorities to whom incidents are to be reported are identified;

[d] organizational officials to whom incidents are to be reported are identified;

[e] identified authorities are notified of incidents; and

[f] identified organizational officials are notified of incidents.

Example

You notice unusual activity on a server and determine a potential security incident has occurred. You open a tracking ticket with the Security Operations Center (SOC), which assigns an incident handler to work the ticket [a]. The handler investigates and documents initial findings, which lead to a determination that unauthorized access occurred on the server [b]. The SOC establishes an incident management team consisting of security, database, network, and system administrators. The team meets daily to update progress and plan courses of action to contain the incident [a]. At the end of the day, the team provides a status report to IT executives [d,f]. Two days later, the team declares the incident contained. The team produces a final report as the database system is rebuilt and placed back into operation.

IR.L2-3.6.3 – INCIDENT RESPONSE TESTING

Test the organizational incident response capability.

Determine if:

[a] the incident response capability is tested.

Example

You decide to conduct an incident response table top exercise that simulates an attacker gaining access to the network through a compromised server. You include relevant IT staff such as security, database, network, and system administrators as participants. You also request representatives from legal, human resources, and communications. You provide a scenario to the group and have prepared key questions aligned with the response plans to guide the exercise. During the exercise, you focus on how the team executes the incident response plan. Afterward, you conduct a debrief with everyone that was involved to provide feedback and develop improvements to the incident response plan [a].

Maintenance (MA)

MA.L2-3.7.1 – PERFORM MAINTENANCE

Perform maintenance on organizational systems.

Example

You are responsible for maintenance activities on your company's machines. This includes regular planned maintenance, unscheduled maintenance, reconfigurations when required, and damage repairs [a]. You know that failing to conduct maintenance activities can impact system security and availability, so you ensure that maintenance is regularly performed. You track all maintenance performed to assist with troubleshooting later if needed.

MA.L2-3.7.2 – SYSTEM MAINTENANCE CONTROL

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Determine if:

[a] tools used to conduct system maintenance are controlled;

[b] techniques used to conduct system maintenance are controlled;

[c] mechanisms used to conduct system maintenance are controlled; and

[d] personnel used to conduct system maintenance are controlled.

Example

You are responsible for maintenance activities on your company's machines. To avoid introducing additional vulnerability into the systems you are maintaining, you make sure that all maintenance tools are approved and their usage is monitored and controlled [a,b]. You ensure the tools are kept current and up-to-date [a]. You and your backup are the only people authorized to use these tools and perform system maintenance [d].

MA.L2-3.7.3 – EQUIPMENT SANITIZATION

Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Determine if:

[a] equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.

Example

You manage your organization's IT equipment. A recent DoD project has been using a storage array to house CUI. Recently, the array has experienced disk issues. After troubleshooting with the vendor, they recommend several drives be replaced in the array. Knowing the drives may contain CUI, you reference NIST 800-88 Rev. 1 and determine a strategy you can implement on the defective equipment – processing the drives with a degaussing unit [a]. Once all the drives have been wiped, you document the action and ship the faulty drives to the vendor.

MA.L2-3.7.4 – MEDIA INSPECTION

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Determine if:

[a] media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.

Example

You have recently been experiencing performance issues on one of your servers. After troubleshooting for much of the morning, the vendor has asked to install a utility that will collect more data from the server. The file is stored on the vendor's FTP server. The support technician gives you the FTP site so you can anonymously download the utility file. You also ask him for a hash of the utility file. As you download the file to your local computer, you realize it is compressed. You unzip the file and perform a manual antivirus scan, which reports no issues [a]. To verify the utility file has not been altered, you run an application to see that the hash from the vendor matches.

MA.L2-3.7.5 – NONLOCAL MAINTENANCE

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Determine if:

[a] multifactor authentication is used to establish nonlocal maintenance sessions via external network connections; and

[b] nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.

Example

You are responsible for maintaining your company's firewall. In order to conduct maintenance while working remotely, you connect to the firewall's management interface and log in using administrator credentials. The firewall then sends a verification request to the multifactor authentication app on your smartphone [a]. You need both of these things to prove your identity [a]. After you respond to the multifactor challenge, you have access to the maintenance interface. When you finish your activities, you shut down the remote connection by logging out and quitting your web browser [b].

MA.L2-3.7.6 – MAINTENANCE PERSONNEL

Supervise the maintenance activities of maintenance personnel without required access authorization.

Determine if:

[a] maintenance personnel without required access authorization are supervised during maintenance activities.

Example

One of your software providers has to come on-site to update the software on your company's computers. You give the individual a temporary logon and password that expires in 12 hours and is limited to accessing only the computers necessary to complete the work [a]. This gives the technician access long enough to perform the update. You monitor the individual's physical and network activity while the maintenance is taking place [a] and revoke access when the job is done.

Media Protection (MP)

MP.L2-3.8.1 – MEDIA PROTECTION

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Determine if:

[a] paper media containing CUI is physically controlled;

[b] digital media containing CUI is physically controlled;

[c] paper media containing CUI is securely stored; and

[d] digital media containing CUI is securely stored.

Example

Your company has CUI for a specific Army contract contained on a USB drive. You store the drive in a locked drawer, and you log it on an inventory [d]. You establish a procedure to check out the USB drive so you have a history of who is accessing it. These procedures help to maintain the confidentiality, integrity, and availability of the data.

MP.L2-3.8.2 – MEDIA ACCESS

Limit access to CUI on system media to authorized users.

Determine if:

[a] access to CUI on system media is limited to authorized users.

Example

Your company has CUI for a specific Army contract contained on a USB drive. In order to control the data, you establish specific procedures for handling the drive. You designate the project manager as the owner of the data and require anyone who needs access to the data to get permission from the data owner [a]. The data owner maintains a list of users that are authorized to access the information. Before an authorized individual can get access to the USB drive that contains the CUI they have to fill out a log and check out the drive. When they are done with the data, they check in the drive and return it to its secure storage location.

MP.L2-3.8.3 – MEDIA DISPOSAL [CUI DATA]

Sanitize or destroy system media containing CUI before disposal or release for reuse.

Determine if:

[a] system media containing CUI is sanitized or destroyed before disposal; and

[b] system media containing CUI is sanitized before it is released for reuse.

Example

As you pack for an office move, you find some old CDs in a file cabinet. You determine that one has information about an old project your company did for the DoD. You shred the CD rather than simply throwing it in the trash [a].

MP.L2-3.8.4 – MEDIA MARKINGS

Mark media with necessary CUI markings and distribution limitations.

Determine if:

[a] media containing CUI is marked with applicable CUI markings; and

[b] media containing CUI is marked with distribution limitations.

Example

You were recently contacted by the project team for a new DoD program. The team said they wanted the CUI in use for the program to be properly protected. When speaking with them, you realize that most of the protections will be provided as part of existing enterprise cybersecurity capabilities. They also mentioned that the project team will use several USB drives to share specific data. You explain that the team must ensure the USB drives are externally marked to indicate the presence of CUI [a]. The project team labels the outside of each USB drive with an appropriate CUI label following NARA guidance [a]. Further, the labels indicate that distribution is limited to those employees supporting the DoD program [a].

MP.L2-3.8.5 – MEDIA ACCOUNTABILITY

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Determine if:

[a] access to media containing CUI is controlled; and

[b] accountability for media containing CUI is maintained during transport outside of controlled areas.

Example

Your team has recently completed configuring a server for a DoD customer. The customer has asked that it be ready to plug in and use. An application installed on the server contains data that is considered CUI. You box the server for shipment using tamper-evident packaging and label it with the specific recipient for the shipment [b]. You select a reputable shipping service so you will get a tracking number to monitor the progress. Once the item is shipped, you send the recipients the tracking number so they can monitor and ensure prompt delivery at their facility.

MP.L2-3.8.6 – PORTABLE STORAGE ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Determine if:

[a] the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.

Example

You manage the backups for file servers in your datacenter. You know that in addition to the company's sensitive information, CUI is stored on the file servers. As part of a broader plan to protect data, you send the backup tapes off site to a vendor. You are aware that your backup software provides the option to encrypt data onto tape. You develop a plan to test and enable backup encryption for the data sent off site. This encryption provides additional protections for the data on the backup tapes during transport and offsite storage [a].

MP.L2-3.8.7 – REMOVEABLE MEDIA

Control the use of removable media on system components.

Determine if:

[a] the use of removable media on system components is controlled.

Example

You are in charge of IT operations. You establish a policy for removable media that includes USB drives [a]. The policy information such as:

- only USB drives issued by the organization may be used; and
- USB drives are to be used for work purposes only [a].

You set up a separate computer to scan these drives before anyone uses them on the network. This computer has anti-virus software installed that is kept up to date.

MP.L2-3.8.8 – SHARED MEDIA

Prohibit the use of portable storage devices when such devices have no identifiable owner.
Determine if:

[a] the use of portable storage devices is prohibited when such devices have no identifiable owner.

Example

You are the IT manager. One day, a staff member reports finding a USB drive in the parking lot. You investigate and learn that there are no labels on the outside of the drive to indicate who might be responsible for it. You send an email to all employees to remind them that IT policies expressly prohibit plugging unknown devices into company computers. You also direct staff members to turn in to the IT help desk any devices that have no identifiable owner [a].

MP.L2-3.8.9 – PROTECT BACKUPS

Protect the confidentiality of backup CUI at storage locations.

Determine if:

[a] the confidentiality of backup CUI is protected at storage locations.

Example

You are in charge of protecting CUI for your company. Because the company's backups contain CUI, you work with IT to protect the confidentiality of backup data. You agree to encrypt all CUI data as it is saved to an external hard drive [a].

Personnel Security (PS)

PS.L2-3.9.1 – SCREEN INDIVIDUALS

Screen individuals prior to authorizing access to organizational systems containing CUI.
Determine if: [a]

individuals are screened prior to authorizing access to organizational systems containing CUI.

Example

You are in charge of security at your organization. You complete standard criminal background and credit checks of all individuals you hire before they can access CUI [a]. Your screening program follows appropriate laws, policies, regulations, and criteria for the level of access required for each position.

PS.L2-3.9.2 – PERSONNEL ACTIONS

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Determine if:

[a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established;

[b] system access and credentials are terminated consistent with personnel actions such as termination or transfer; and

[c] the system is protected during and after personnel transfer actions.

Example 1

You are in charge of IT operations. Per organizational policies, when workers leave the company, you remove them from any physical CUI access lists. If you are not their supervisor, you contact their supervisor or human resources immediately and ask them to:

• turn in the former employees' computers for proper handling

• inform help desk or system administrators to have the former employees' system access revoked;

• retrieve the former employees' identification and access cards; and

• have the former employees attend an exit interview where you or human resources remind them of their obligations to not discuss CUI [b].

Example 2

An employee transfers from one working group in your company to another. Human resources team notifies IT of the transfer date, and the employee's new manager follows procedure by submitting a ticket to the IT help desk to provide information on the access rights the employee will require in their new role. IT implements the rights for the new position and revokes the access for the prior position on the official date of the transfer [c].

Physical Protection (PE)

PE.L2-3.10.1 – LIMIT PHYSICAL ACCESS [CUI DATA]

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

Determine if:

[a] authorized individuals allowed physical access are identified;

[b] physical access to organizational systems is limited to authorized individuals;

[c] physical access to equipment is limited to authorized individuals; and

[d] physical access to operating environments is limited to authorized individuals.[27]

Example

You manage a DoD project that requires special equipment used only by project team members [b,c]. You work with the facilities manager to put locks on the doors to the areas where the equipment is stored and used [b,c,d]. Project team members are the only individuals issued with keys to the space. This restricts access to only those employees who work on the DoD project and require access to that equipment.

PE.L2-3.10.2 – MONITOR FACILITY

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

[27] NIST SP 800-171A

Determine if:

[a] the physical facility where organizational systems reside is protected;

[b] the support infrastructure for organizational systems is protected;

[c] the physical facility where organizational systems reside is monitored; and

[d] the support infrastructure for organizational systems is monitored.

Example

You are responsible for protecting your IT facilities. You install video cameras at each entrance and exit, connect them to a video recorder, and show the camera feeds on a display at the reception desk [c,d]. You also make sure there are secure locks on all entrances, exits, and windows to the facilities [a,b].

PE.L2-3.10.3 – ESCORT VISITORS [CUI DATA]

Escort visitors and monitor visitor activity.

Determine if:

[a] visitors are escorted; and

[b] visitor activity is monitored.

Example

Coming back from a meeting, you see the friend of a coworker walking down the hallway near your office. You know this person well and trust them, but are not sure why they are in the building. You stop to talk, and the person explains that they are meeting a coworker for lunch, but cannot remember where the lunchroom is. You walk the person back to the reception area to get a visitor badge and wait until someone can escort them to the lunch room [a]. You report this incident and the company decides to install a badge reader at the main door so visitors cannot enter without an escort [a].

PE.L2-3.10.4 – PHYSICAL ACCESS LOGS [CUI DATA]

Maintain audit logs of physical access.

Determine if:

[a] audit logs of physical access are maintained.

Example

You and your coworkers like to have friends and family join you for lunch at the office on Fridays. Your small company has just signed a contract with the DoD, however, and you now need to document who enters and leaves your facility. You work with the reception staff to ensure that all non-employees sign in at the reception area and sign out when they leave [a]. You retain those paper sign-in sheets in a locked filing cabinet for one year. Employees receive badges or key cards that enable tracking and logging access to company facilities.

PE.L2-3.10.5 – MANAGE PHYSICAL ACCESS [CUI DATA]

Control and manage physical access devices.

Determine if:

[a] physical access devices are identified;

[b] physical access devices are controlled; and

[c] physical access devices are managed.

Example

You are a facility manager. A team member retired today and returns their company keys to you. The project on which they were working requires access to areas that contain equipment with CUI. You receive the keys, check your electronic records against the serial numbers on the keys to ensure all have been returned, and mark each key returned [c].

PE.L2-3.10.6 – ALTERNATIVE WORK SITES

Enforce safeguarding measures for CUI at alternate work sites.

Determine if:

[a] safeguarding measures for CUI are defined for alternate work sites; and

[b] safeguarding measures for CUI are enforced for alternate work sites.

Example

Many of your company's project managers work remotely as they often travel to sponsor locations or even work from home. Because the projects on which they work require access to CUI, you must ensure the same level of protection is afforded as when they work in the office. You ensure that each laptop is deployed with patch management and anti-virus software protection [b]. Because data may be stored on the local hard drive, you have enabled full-disk encryption on their laptops [b]. When a remote staff member needs access to the internal network you require VPN connectivity that also disconnects the laptop from the remote network (i.e., prevents split tunneling) [b]. The VPN requires multifactor authentication to verify remote users are who they claim to be [b].

Risk Assessment (RA)

RA.L2-3.11.1 – RISK ASSESSMENTS

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Determine if:

[a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined; and

[b] risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

Example

You are a system administrator. You and your team members are working on a big government contract requiring you to store CUI. As part of your periodic (e.g., annual) risk assessment exercise, you evaluate the new risk involved with storing CUI [a,b]. When conducting the assessment you consider increased legal exposure, financial requirements of safeguarding CUI, potentially elevated attention from external attackers, and other factors. After determining how storing CUI affects your overall risk profile, you use that as a basis for a conversation on how that risk should be mitigated.

RA.L2-3.11.2 – VULNERABILITY SCAN

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Determine if:

[a] the frequency to scan for vulnerabilities in organizational systems and applications is defined;

[b] vulnerability scans are performed on organizational systems with the defined frequency;

[c] vulnerability scans are performed on applications with the defined frequency;

[d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified; and

[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

Example

You are a system administrator. Your organization has assessed its risk and determined that it needs to scan for vulnerabilities in systems and applications once each quarter [a]. You conduct some tests and decide that it is important to be able to schedule scans after standard business hours. You also realize that you have remote workers and that you will need to be sure to scan their remote computers as well [b]. After some final tests, you integrate the scans into normal IT operations, running as scheduled [b,c]. You verify that the scanner application receives the latest updates on vulnerabilities and that those are included in future scans [d,e].

Example

You are a system administrator. Each quarter you receive a list of vulnerabilities generated by your company's vulnerability scanner [a]. You prioritize that list and note which vulnerabilities should be targeted as soon as possible as well as which vulnerabilities you can safely defer addressing at this time. You document the reasoning behind accepting the risk of the unremediated flaws and note to continue to monitor these vulnerabilities in case you need to revise the decision at a later date [b].

Security Assessment (CA)

CA.L2-3.12.1 – SECURITY CONTROL ASSESSMENT

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Determine if:

[a] the frequency of security control assessments is defined; and

[b] security controls are assessed with the defined frequency to determine if the controls are effective in their application.

Example

You are in charge of IT operations. You need to ensure that the security controls implemented within the system are achieving their objectives [b]. Taking the requirements outlined in your SSP as a guide, you conduct annual written reviews of the security controls to ensure they meet your organization's needs. When you find controls that do not meet requirements, you propose updated or new controls, develop a written implementation plan, document new risks, and execute the changes.

CA.L2-3.12.2 – OPERATIONAL PLAN OF ACTION

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Determine if:

[a] deficiencies and vulnerabilities to be addressed by the plan of action are identified;

[b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities; and

[c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Example

As IT director, one of your duties is to develop action plans when you discover that your company is not meeting security requirements or when a security issue arises [b]. A recent vulnerability scan identified several items that need to be addressed so you develop a plan to fix them [b]. Your plan identifies the people responsible for fixing the issues, how to do it, and when the remediation will be completed [b]. You also define how to verify that the person responsible has fixed the vulnerability [b]. You document this in an operational plan of action that is updated as milestones are reached [b]. You have a separate resource review the modifications after they have been completed to ensure the plan has been implemented correctly [c].

CA.L2-3.12.3 – SECURITY CONTROL MONITORING

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Determine if:

[a] security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Example

You are responsible for ensuring your company fulfills all cybersecurity requirements for its DoD contracts. You review those requirements and the security controls your company has put in place to meet them. You then create a plan to evaluate each control regularly over the next

year. You mark several controls to be evaluated by a third-party security assessor. You assign other IT resources in the organization to evaluate controls within their area of responsibility. To ensure progress you establish recurring meetings with the accountable IT staff to assess continuous monitoring progress, review security information, evaluate risks from gaps in continuous monitoring, and produce reports for your management [a].

CA.L2-3.12.4 – SYSTEM SECURITY PLAN

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Determine if:

[a] a system security plan is developed;

[b] the system boundary is described and documented in the system security plan;

[c] the system environment of operation is described and documented in the system security plan;

[d] the security requirements identified and approved by the designated authority as non-applicable are identified;

[e] the method of security requirement implementation is described and documented in the system security plan;

[f] the relationship with or connection to other systems is described and documented in the system security plan;

[g] the frequency to update the system security plan is defined; and

[h] system security plan is updated with the defined frequency.

Example

You are in charge of system security. You develop an SSP and have senior leadership formally approve the document [a]. The SSP explains how your organization handles CUI and defines how that data is stored, transmitted, and protected [d,e]. The criteria outlined in the SSP is used to guide configuration of the network and other information resources to meet your company's goals. Knowing that it is important to keep the SSP current, you establish a policy that requires a formal review and update of the SSP each year [g,h].

System and Communications Protection (SC)

SC.L2-3.13.1 – BOUNDARY PROTECTION [CUI DATA]

Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Determine if:

[a] the external system boundary is defined;

[b] key internal system boundaries are defined;

[c] communications are monitored at the external system boundary;

[d] communications are monitored at key internal boundaries;

[e] communications are controlled at the external system boundary;

[f] communications are controlled at key internal boundaries;

[g] communications are protected at the external system boundary; and

[h] communications are protected at key internal boundaries.

Example

You are setting up the new network and want to keep your company's information and resources safe. You start by sketching out a simple diagram that identifies the external boundary of your network and any internal boundaries that are needed [a,b]. The first piece of equipment you install is the firewall, a device to separate your internal network from the internet. The firewall also has a feature that allows you to block access to potentially malicious websites, and you configure that service as well [a,c,e,g]. Some of your coworkers complain that they cannot get onto certain websites [c,e,g]. You explain that the new network blocks websites that are known for spreading malware. The firewall sends you a daily digest of blocked activity so that you can monitor the system for attack trends [c,d].

SC.L2-3.13.2 – SECURITY ENGINEERING

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Determine if:

[a] architectural designs that promote effective information security are identified;

[b] software development techniques that promote effective information security are identified; [c] systems engineering principles that promote effective information security are identified;

[d] identified architectural designs that promote effective information security are employed;

[e] identified software development techniques that promote effective information security are employed; and

[f] identified systems engineering principles that promote effective information security are employed.

Example

You are responsible for developing strategies to protect data and harden your infrastructure. You are on a team responsible for performing a major upgrade to a legacy system. You refer to your documented security engineering principles [c]. Reviewing each, you decide which are appropriate and applicable [c]. You apply the chosen designs and principles when creating your design for the upgrade [f].

You document the security requirements for the software and hardware changes to ensure the principles are followed. You review the upgrade at critical points in the workflow to ensure the requirements are met. You assist in updating the policies covering the use of the upgraded system so user behavior stays aligned with the principles.

SC.L2-3.13.3 – ROLE SEPARATION

Separate user functionality from system management functionality.

Determine if:

[a] user functionality is identified;

[b] system management functionality is identified; and

[c] user functionality is separated from system management functionality.

Example

As a system administrator, you are responsible for managing a number of core systems. Policy prevents you from conducting any administration from the computer or system account you use for day-to-day work [a,b]. The servers you manage also are isolated from the main corporate network. To work with them you use a special unique account to connect to a "jump" server that has access to the systems you routinely administer.

SC.L2-3.13.4 – SHARED RESOURCE CONTROL

Prevent unauthorized and unintended information transfer via shared system resources.
Determine if:

[a] unauthorized and unintended information transfer via shared system resources is prevented.

Example

You are a system administrator responsible for creating and deploying the system hardening procedures for your company's computers. You ensure that the computer baselines include software patches to prevent attackers from exploiting flaws in the processor architecture to read data (e.g., the Meltdown and Spectre exploits). You also verify that the computer operating system is configured to prevent users from accessing other users' folders [a].

SC.L2-3.13.5 – PUBLIC-ACCESS SYSTEM SEPARATION [CUI DATA]

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Determine if:

[a] publicly accessible system components are identified; and

[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks.

Example

The head of recruiting at your company wants to launch a website to post job openings and allow the public to download an application form [a]. After some discussion, your team realizes it needs to use a firewall to create a perimeter network to do this [b]. You host the server separately from the company's internal network and make sure the network on which it resides is isolated with the proper firewall rules [b].

SC.L2-3.13.6 – NETWORK COMMUNICATION BY EXCEPTION

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Determine if:

[a] network communications traffic is denied by default; and

[b] network communications traffic is allowed by exception.

Example

You are setting up a new environment to house CUI. To properly isolate the CUI network, you install a firewall between it and other networks and set the firewall rules to deny all traffic [a]. You review each service and application that runs in the new environment and determine that you only need to allow http and https traffic outbound [b]. You test the functionality of the required services and make some needed adjustments, then comment each firewall rule so there is documentation of why it is required. You review the firewall rules on a regular basis to make sure no unauthorized changes were made.

SC.L2-3.13.7 – SPLIT TUNNELING

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Determine if:

[a] remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Example

You are a system administrator responsible for configuring the network to prevent remote users from using split tunneling. You review the configuration of remote user laptops. You discover that remote users are able to access files, email, database and other services through the VPN connection while also being able to print and access resources on their local network. You change the configuration settings for all company computers to disable split tunneling [a]. You test a laptop that has had the new hardening procedures applied and verify that all traffic from the laptop is now routed through the VPN connection.

SC.L2-3.13.8 – DATA IN TRANSIT

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Determine if:

[a] cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified;

[b] alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified; and

[c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.

Example

You are a system administrator responsible for configuring encryption on all devices that contain CUI. Because your users regularly store CUI on laptops and take them out of the office, you encrypt the hard drives with a FIPS-validated encryption tool built into the operating system. For users who need to share CUI, you install a Secure FTP server to allow CUI to be transmitted in a compliant manner [a]. You verify that the server is using a FIPSvalidated encryption module by checking the NIST Cryptographic Module Validation Program website [c]. You turn on the "FIPS Compliance" setting for the server during configuration because that is what is required for this product in order to use only FIPSvalidated cryptography [c].

SC.L2-3.13.9 – CONNECTIONS TERMINATION

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Determine if:

[a] a period of inactivity to terminate network connections associated with communications sessions is defined;

[b] network connections associated with communications sessions are terminated at the end of the sessions; and

[c] network connections associated with communications sessions are terminated after the defined period of inactivity.

Example

You are an administrator of a server that provides remote access. Your company's policies state that network connections must be terminated after being idle for 60 minutes [a]. You edit the server configuration file and set the timeout to 60 minutes and restart the remote access software [c]. You test the software and verify that the connection is terminated appropriately.

SC.L2-3.13.10 – KEY MANAGEMENT

Establish and manage cryptographic keys for cryptography employed in organizational systems. Determine if:

[a] cryptographic keys are established whenever cryptography is employed; and

[b] cryptographic keys are managed whenever cryptography is employed.

Example 1

You are a system administrator responsible for providing key management. You have generated a public-private key pair to exchange CUI [a]. You require all system administrators to read the

key management policy before you allow them to install the private key on their machines [b]. No one else is allowed to know or have a copy of the private key per the policy. You provide the public key to the other parties who will be sending you CUI and test the Public Key Infrastructure (PKI) to ensure the encryption is working [a]. You set a revocation period of one year on all your certificates per organizational policy [b].

Example 2

You encrypt all of your company's computers using the disk encryption utility built into the operating system. As you configure encryption on each device, it generates a cryptographic key. You associate each key with the correct computer in your inventory spreadsheet and restrict access to the spreadsheet to the system administrators whose work role requires them to manage the computers [b].

SC.L2-3.13.11 – CUI ENCRYPTION

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Determine if:

[a] FIPS-validated cryptography is employed to protect the confidentiality of CUI.

Example

You are a system administrator responsible for deploying encryption on all devices that contain CUI. You must ensure that the encryption you use on the devices is FIPS-validated cryptography [a]. An employee informs you of a need to carry a large volume of CUI offsite and asks for guidance on how to do so. You provide the user with disk encryption software that you have verified via the NIST website that uses a CMVP-validated encryption module [a]. Once the encryption software is active, the user copies the CUI data onto the drive for transport.

SC.L2-3.13.12 – COLLABORATIVE DEVICE CONTROL

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Determine if:

[a] collaborative computing devices are identified;

[b] collaborative computing devices provide indication to users of devices in use; and

[c] remote activation of collaborative computing devices is prohibited.

Example

A group of remote employees at your company routinely collaborate using cameras and microphones attached to their computers [a]. To prevent the misuse of these devices, you disable the ability to turn on cameras or microphones remotely [c]. You ensure the machines alert users when the camera or microphone are in use with a light beside the camera and an onscreen notification [b]. Although remote activation is blocked, this enables users to see if the devices are active.

SC.L2-3.13.13 – MOBILE CODE

Control and monitor the use of mobile code.

Determine if:

[a] use of mobile code is controlled; and

[b] use of mobile code is monitored.

Example

Your company has decided to prohibit the use of Flash, ActiveX, and Java plug-ins for web browsers on all of its computers [a]. To enforce this policy you configure the computer baseline configuration to disable and deny the execution of mobile code [a]. You implement an exception process to re-enable mobile code execution only for those users with a legitimate business need [a].

One department complains that a web application they need to perform their job no longer works. You meet with them and verify that the web application uses ActiveX in the browser. You submit a change request with the Change Review Board. Once the change is approved, you reconfigure the department's computers to allow the running of ActiveX in the browser. You also configure the company firewall to alert you if ActiveX is used by any website but the allowed one [b]. You set a reminder for yourself to check in with the department at the end of the year to verify they still need that web application.

SC.L2-3.13.14 – VOICE OVER INTERNET PROTOCOL

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Determine if:

[a] use of Voice over Internet Protocol (VoIP) technologies is controlled; and

[b] use of Voice over Internet Protocol (VoIP) technologies is monitored.

Example

You are a system administrator responsible for the VoIP system. You configure VoIP for new users after being notified that they have signed the Acceptable Use Policy for VoIP technology [a]. You verify that the VoIP solution is configured to use encryption and have enabled requirements for passwords on voice mailboxes and on phone extension management. You

require phone system administrators to log in using multifactor authentication when managing the system [a]. You add the VoIP software to the list of applications that are patched monthly as needed [a,b]. Finally, you configure the VoIP system to send logs to your log aggregator so that they can be correlated with those from other systems and examined for signs of suspicious activity [b].

SC.L2-3.13.15 – COMMUNICATIONS AUTHENTICITY

Protect the authenticity of communications sessions.

Determine if:

[a] the authenticity of communications sessions is protected.

Example

You are a system administrator responsible for ensuring that the two-factor user authentication mechanism for the servers is configured correctly. You purchase and maintain the digital certificate and replace it with a new one before the old one expires. You ensure the TLS configuration settings on the web servers, VPN solution, and other components that use TLS are correct, using secure settings that address risks against attacks on the encrypted sessions [a].

SC.L2-3.13.16 – DATA AT REST

Protect the confidentiality of CUI at rest.

Determine if:

[a] the confidentiality of CUI at rest is protected.

Example 1

Your company has a policy stating CUI must be protected at rest and you work to enforce that policy. You research Full Disk Encryption (FDE) products that meet the FIPS encryption requirement. After testing, you deploy the encryption to all computers to protect CUI at rest [a].

Example 2

You have used encryption to protect the CUI on most of the computers at your company, but you have some devices that do not support encryption. You create a policy requiring these devices to be signed out when needed, stay in possession of the signer when checked out, and to be signed back in and locked up in a secured closet when the user is done with the device [a]. At the end of the day each Friday, you audit the sign-out sheet and make sure all devices are returned to the closet.

System and Information Integrity (SI)

SI.L2-3.14.1 – FLAW REMEDIATION [CUI DATA]

Identify, report, and correct system flaws in a timely manner.

Determine if:

[a] the time within which to identify system flaws is specified;

[b] system flaws are identified within the specified time frame;

[c] the time within which to report system flaws is specified;

[d] system flaws are reported within the specified time frame;

[e] the time within which to correct system flaws is specified; and

[f] system flaws are corrected within the specified time frame.

Example

You know that software vendors typically release patches, service packs, hot fixes, etc. and want to make sure your software is up to date. You develop a policy that requires checking vendor websites for flaw notifications every week [a]. The policy further requires that those flaws be assessed for severity and patched on end-user computers once each week and servers once each month [c,e]. Consistent with that policy, you configure the system to check for updates weekly or daily depending on the criticality of the software [b,e]. Your team reviews available updates and implements the applicable ones according to the defined schedule [f].

SI.L2-3.14.2 – MALICIOUS CODE PROTECTION [CUI DATA]

Provide protection from malicious code at designated locations within organizational systems.

Determine if:

[a] designated locations for malicious code protection are identified; and

[b] protection from malicious code at designated locations is provided.

Example

You are buying a new computer and want to protect your company's information from viruses, spyware, etc. You buy and install anti-malware software [a,b].

SI.L2-3.14.3 – SECURITY ALERTS & ADVISORIES

Monitor system security alerts and advisories and take action in response.

Determine if:

[a] response actions to system security alerts and advisories are identified;

[b] system security alerts and advisories are monitored; and

[c] actions in response to system security alerts and advisories are taken.

Example

You monitor security advisories each week. You review the alert emails and online subscription service alerts to determine which ones apply [b]. You create a list of the applicable alerts and research what steps you need to take to address them. Next, you generate a plan that you review with your change management group so that the work can be scheduled [c].

SI.L2-3.14.4 – UPDATE MALICIOUS CODE PROTECTION [CUI DATA]

Update malicious code protection mechanisms when new releases are available.

Determine if:

[a] malicious code protection mechanisms are updated when new releases are available.

Example

You have installed anti-malware software to protect a computer from malicious code. Knowing that malware evolves rapidly, you configure the software to automatically check for malware definition updates every day and update as needed [a].

SI.L2-3.14.5 – SYSTEM & FILE SCANNING [CUI DATA]

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Determine if:

[a] the frequency for malicious code scans is defined;

[b] malicious code scans are performed with the defined frequency; and

[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

Example

You work with your company's email provider to enable enhanced protections that will scan all attachments to identify and quarantine those that may be harmful prior to a user opening them [c]. In addition, you configure antivirus software on each computer to scan for malicious code every day [a,b]. The software also scans files that are downloaded or copied from removable media such as USB drives. It quarantines any suspicious files and notifies the security team [c].

SI.L2-3.14.6 – MONITOR COMMUNICATIONS FOR ATTACKS

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Determine if:

[a] the system is monitored to detect attacks and indicators of potential attacks;

[b] inbound communications traffic is monitored to detect attacks and indicators of potential attacks; and

[c] outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

Example

It is your job to look for known indicators of attack or anomalous activity within your systems and communications traffic [a,b,c]. Because these indicators can show up in a variety of places on your network, you have created a checklist of places to check each week. These include the office firewall logs, the audit logs of the file server where CUI is stored, and the connection log for your VPN gateway [b]. You conduct additional reviews when you find an indicator, or something that does not perform as it should [a].

SI.L2-3.14.7 – IDENTIFY UNAUTHORIZED USE

Identify unauthorized use of organizational systems.

Determine if:

[a] authorized use of the system is defined; and [b] unauthorized use of the system is identified.

Example 1

You are in charge of IT operations. You need to ensure that everyone using an organizational system is authorized to do so and conforms to the written authorized use policy. To do this, you deploy an application that monitors user activity and records the information for later analysis. You review the data from this application for signs of activity that does not conform to the acceptable use policy [a,b].

Example 2

You are alerted through your Intrusion Detection System (IDS) that one of your users is connecting to a server that is from a high-risk domain (based on your commercial domain reputation service). You investigate and determine that it's not the user, but instead an unauthorized connection attempt [b]. You add the domain to your list of blocked domains to prevent connections in the future.

Attesting your Score on SPRS

Overview

This checklist walks your organization through **CMMC Level 2 self-attestation**, including required registrations, role setup, documentation, and submission to the DoD.

Company Registration & System Access

Register in SAM.gov

Purpose: Required to do business with the U.S. Government.

Actions:

- Register or verify your entity at **SAM.gov**
- Obtain a valid **CAGE Code**
- Confirm registration is **Active**

PIEE Registration & Role Assignment

Register in PIEE (Procurement Integrated Enterprise Environment)

Purpose: Provides access to systems required for CMMC compliance and SPRS submission.

Actions:

- Add Your CAGE Code to the PIEE Vendor Group Structure by Contacting the PIEE Help Desk by phone or email: 1-866-618-5988
- A company representative must request your CAGE Code to be added to a Vendor Group in the Procurement Integrated Enterprise Environment (PIEE).
- Provide your CAGE Code and desired Group Name. If you don't specify a Group Name, one will be assigned based on your CAGE Code or company name.
- Go to PIEE and click **Register**
- Select organization type:
    - **Vendor** OR
    - **Contractor** (either is acceptable)

Assign Contractor Administrator Manager (CAM) *(Done During Registration)*

Important:
The **CAM is designated during the PIEE registration process**

Requirements:

- Designate **one primary individual**
- This person should:
  - Be responsible for IT or cybersecurity
  - Serve as the main compliance point of contact

Responsibilities:

- Manage PIEE account and user roles
- Oversee SPRS submissions
- Maintain compliance documentation

Complete PIEE Registration

- Finish all required fields and organization setup
- Confirm account activation

Additional Role Configuration *(Done After Registration)*

Assign Cyber Vendor User Role

Purpose: Enables access to SPRS and cybersecurity modules.

Actions:

- Assign **Cyber Vendor User role** within PIEE
- Recommended: assign to the **same person as CAM**

Verify SPRS Access

Purpose: SPRS is where CMMC self-assessment scores are submitted.

Actions:

- Log into PIEE dashboard
- Confirm **SPRS (Supplier Performance Risk System)** appears
- If not:
  - Log out and back in

- Verify correct role assignment

CMMC Level 2 – Security Self-Assessment

Required Security Documentation

Create System Security Plan (SSP)

Purpose: Documents your security controls and system environment.

Include:

- System scope and boundaries
- Hardware/software inventory
- Security controls in place
- Data handling processes (FCI)
- Access control methods

Create Incident Response Plan (IRP)

Purpose: Defines how your organization handles cybersecurity incidents.

Include:

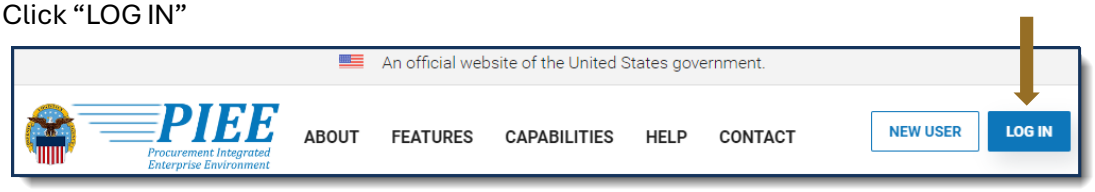
- Incident definitions
- Roles and responsibilities
- Response procedures
- Reporting requirements
- Key contacts

SPRS Submission & Attestation[28]

1. **PIEE Access:** A "SPRS Cyber Vendor User" role is required to enter CMMC Assessment information. PIEE Access Instructions: https://www.sprs.csd.disa.mil/access.htm

2. SPRS Application and Module Access:
   a. PIEE landing page: https://piee.eb.mil/piee-landing/

   b. Click "LOG IN"

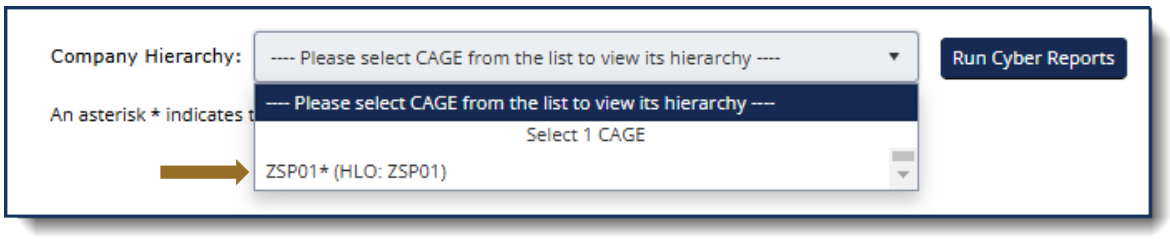


Screenshot Dtd 09 JAN 2024

   c. Select **SPRS**:

   d. Select **Cyber Reports (CMMC & NIST)**:

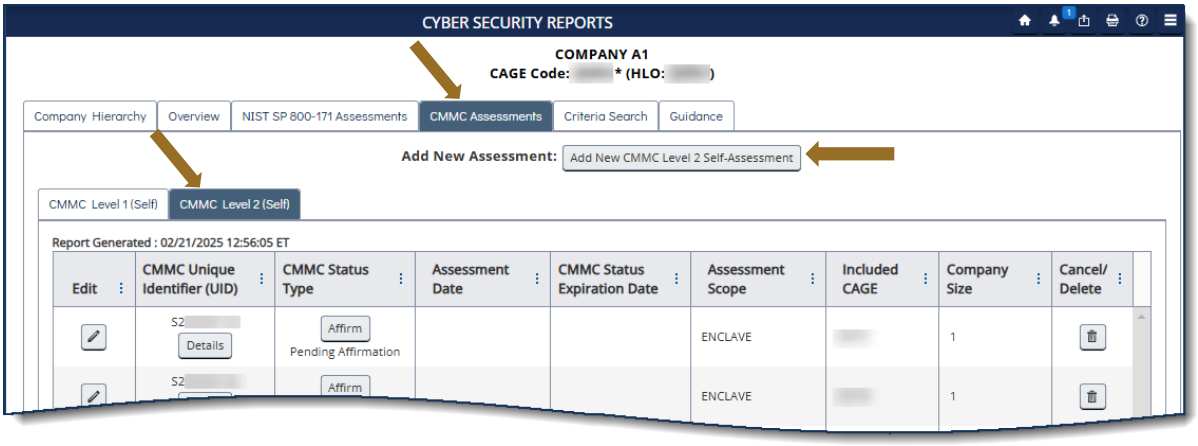
3. **Cyber Reports (CMMC & NIST):** Select the desired Hierarchy, identified by the HLO, from the drop down and select Run Cyber Reports button.



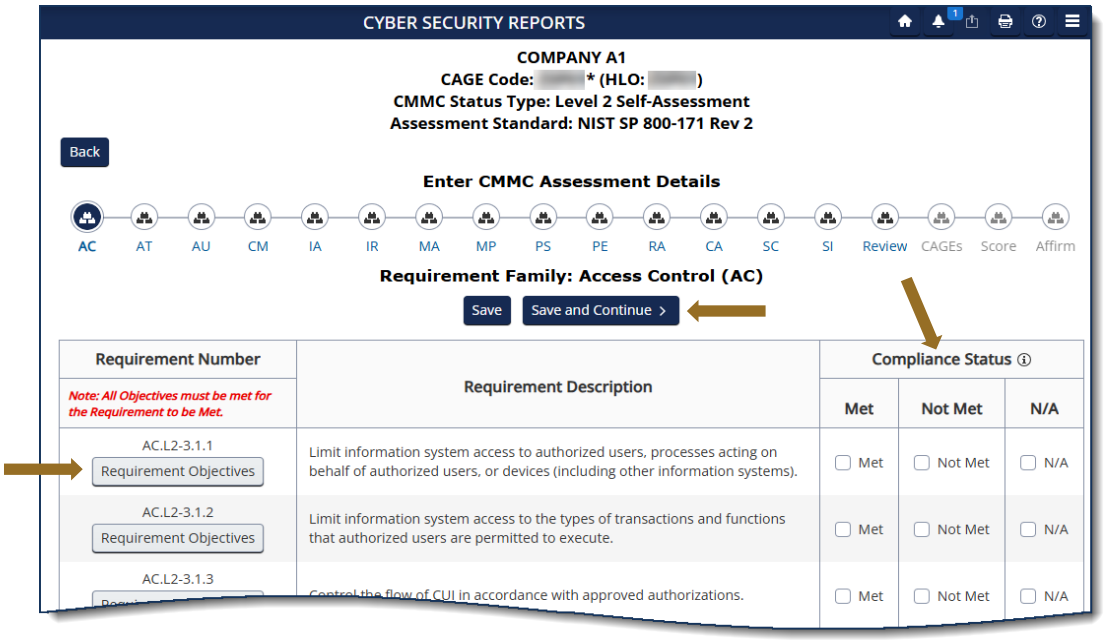
NOTE: An asterisk * indicates the user has the SPRS Cyber Vendor User role (access to add/edit/delete)

[28] CMMC LEVEL 2 SELF-ASSESSMENT QUICK ENTRY GUIDE VERSION 4.0

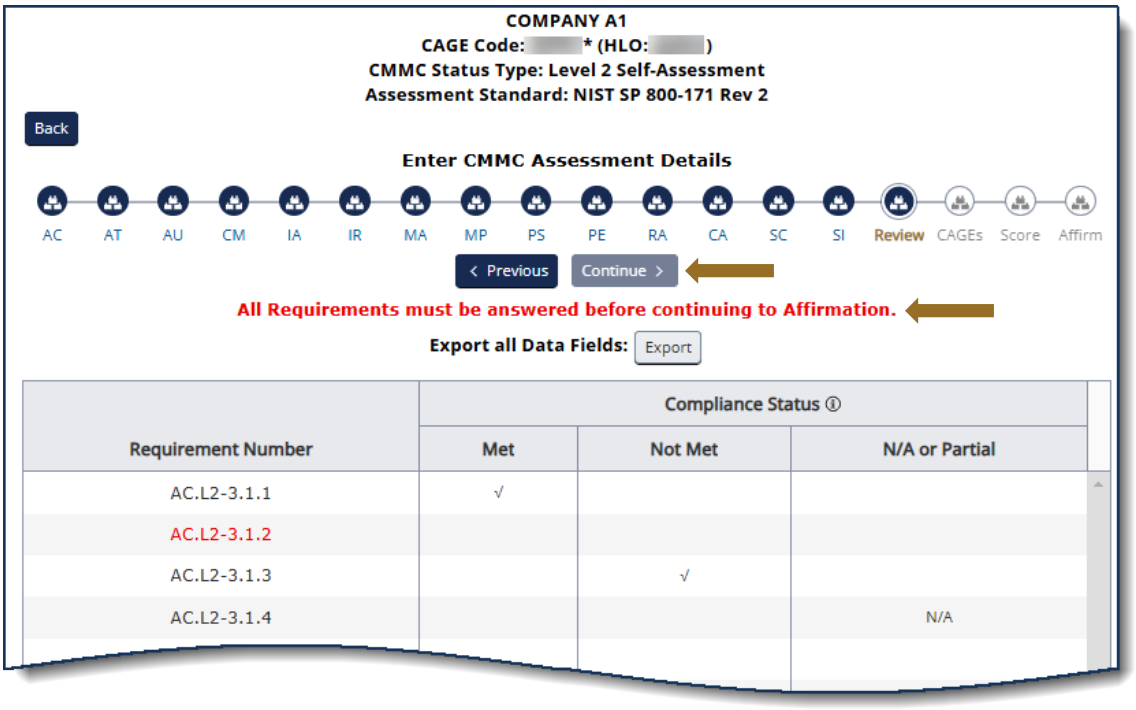
3.1 Add New CMMC Level 2 Self-Assessment: Within the CMMC Assessments and CMMC Level 2 (Self) tabs, select "Add New Level 2 CMMC Self-Assessment".



3.2 Enter Assessment Details: Enter assessment data; review Requirement Objectives to each Requirement Number by selecting the Requirement Objectives button. Select the applicable Compliance Status. Select Save and Continue to navigate through each Requirement Family.



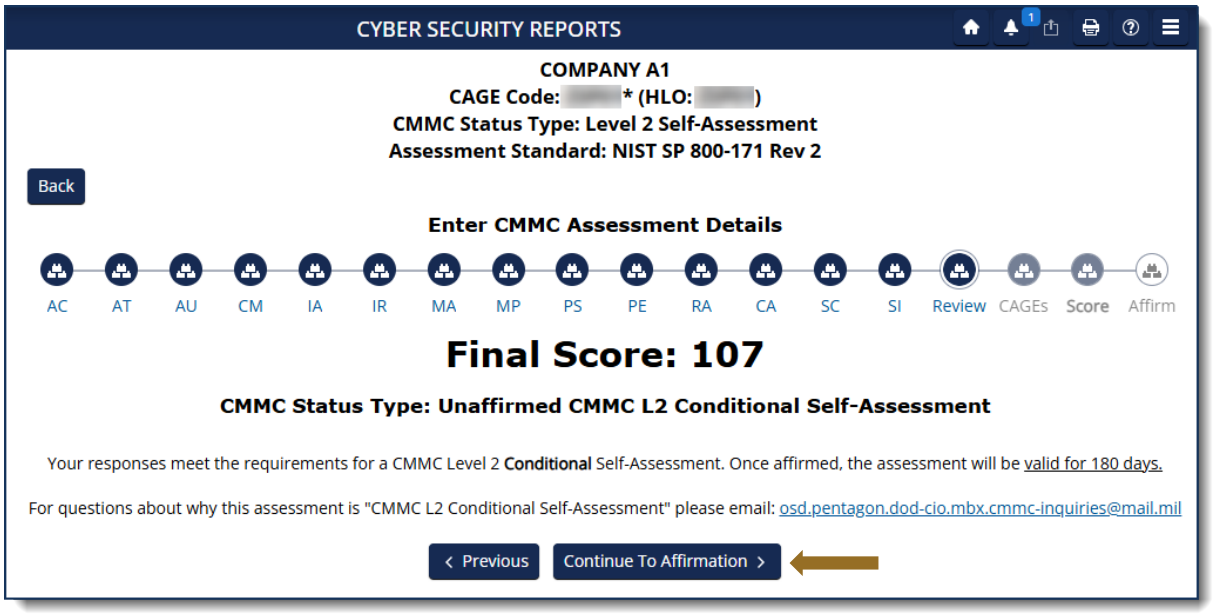
3.3 Review Assessment Details: Answers to Requirements must be complete prior to continuing.



3.4 Additional Assessment Details: Add Assessing Scope, Employee Count, and Included CAGE(s) as required. Select the "Open CAGE Hierarchy" button to add CAGEs or enter comma delimited CAGEs in the data field provided. Select "Save and Continue."

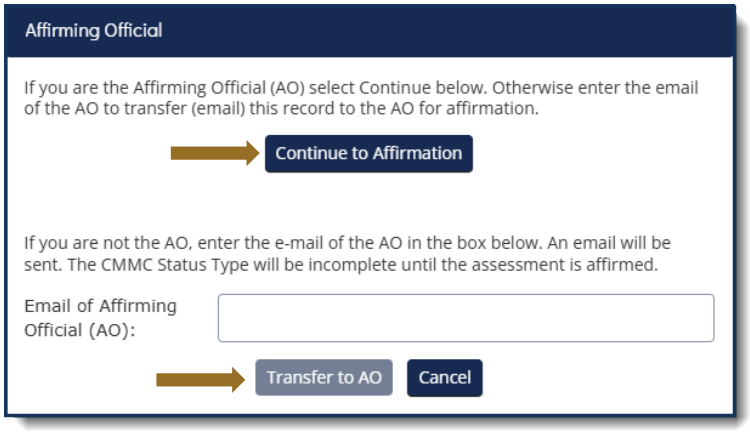
NOTE: CAGE Hierarchy data is imported from the System for Award Management (SAM). Users are unable to add CAGEs that are not part of their company hierarchy.

3.5 Score: Only CMMC L2 Conditional (score = 88 to 109) and Final Self-Assessments (score = 110) can be affirmed.

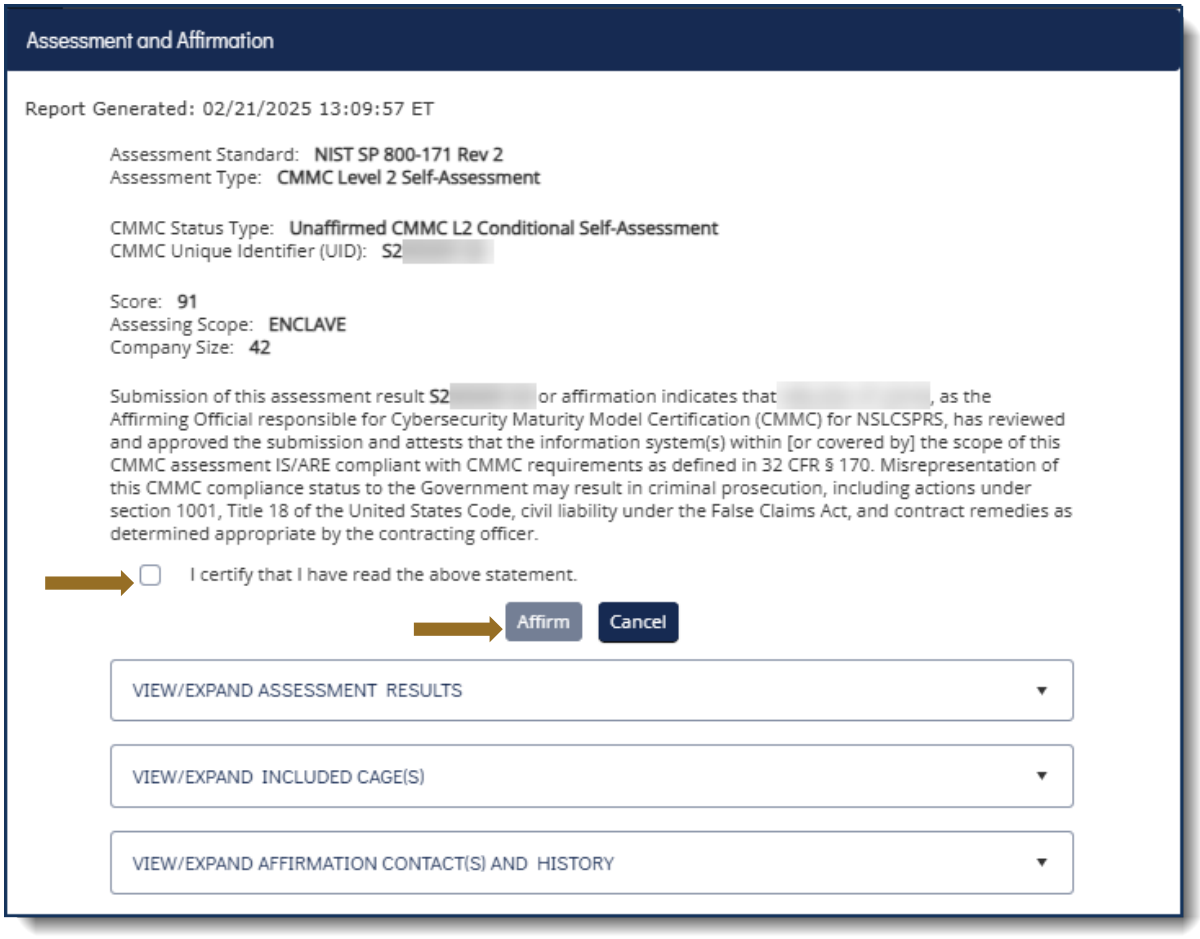


NOTE: If a requirement is not able to be subject to a Plan of Action and Milestones (POA&M), then the Status Type will be No CMMC Status regardless of score.

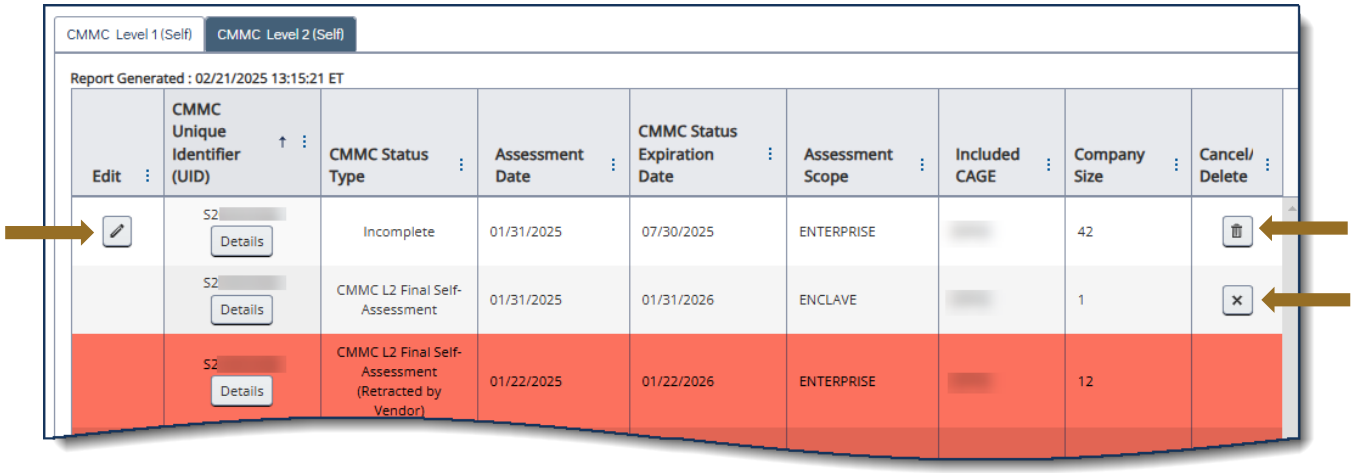
3.6 Transfer to Affirming Official (AO): If the user entering the assessment is not the AO, the assessment can be forwarded via email, to the AO by entering their email and selecting "Transfer to AO".



3.7 Affirm the Assessment: Review the assessment details, certify review of the affirmation statement, and select “Affirm”.



3.8 Assessment Edit/Cancel/Delete: A Cyber Vendor User may Edit, Cancel, or Delete certain CMMC Status Types. Select the available icon to complete the action.



NOTE: A “CMMC L2 Conditional Level 2 Self-Assessment” is valid for 180 days.

A “CMMC L2 Final Level 2 Self-Assessment”, with annual affirmations verifying compliance, is valid for 3 years.”