CMMC Level 2:

You May Be Closer Than You Think

Published by Virtru, with contributors Mark DeBry, Lead CMMC Certified Assessor (LCCA), CCP, & CCA Instructor at 1st Defense CMMC; Juan Salinas, CCP at Virtru; and Andrew Lynch

The Number That Scares Everyone

CMMC Level 2 isn't assessed at the 110 security requirements level, but those requirements are evaluated through 320 individual assessment objectives. To receive MET for a requirement, all applicable objectives for that requirement must be satisfied.

If you've spent any time looking at CMMC Level 2, you've probably had a moment where the scope felt overwhelming, and understandably so, but it's critical you get it right before doing anything else.

But here's what often gets lost in the noise: most organizations pursuing CMMC Level 2 certification already have a significant portion of what they need.

The tools are often already there. What's missing is understanding what each requirement is truly asking for, configuring the technology appropriately, documenting how the requirement is met, and being able to demonstrate that it is working.

Beyond that, the language in the official L2 Assessment Guide can seem confusing to someone who doesn't have a compliance background. This guide is intended to help with that and put some of it into plain text – for the average person.

What CMMC Level 2 Actually Covers

CMMC Level 2 incorporates the 110 security requirements of NIST SP 800-171 Rev. 2 and 320 assessment objectives in NIST SP 800-171a, organized across 14 security requirement families, which CMMC commonly refers to as domains.

Access Control (AC): Who can access what, from where, and under what conditions. This includes everything from approved user lists to how remote sessions are managed.

Awareness and Training (AT): Do your people know what they are responsible for protecting and how? This domain is almost entirely a people and process exercise.

Audit and Accountability (AU): Are your systems logging the right things, and can you trace any action back to a specific individual? This is about what you capture, how long you keep it, and whether you can use it.

Configuration Management (CM): Are your systems built and maintained with a documented, secure baseline? This covers everything from hardened configurations to how you manage system changes.

Identification and Authentication (IA): Can you verify that users, devices, and processes are who they claim to be? MFA, password policies, and unique account requirements all live here.

Incident Response (IR): When something goes wrong, do you have a real plan — and can you execute it? The assessor wants to see an operational capability, not just a document.

Maintenance (MA): Is system maintenance controlled, documented, and performed safely? This includes how you handle remote maintenance, outside vendors, and equipment that leaves the building.

Media Protection (MP): Are physical and digital media containing sensitive data properly secured, labeled, and disposed of? This includes paper documents, not just drives.

Personnel Security (PS): Are the people with access to sensitive systems screened before they start and properly offboarded when they leave?

Physical Protection (PE): Are your facilities, equipment, and supporting infrastructure physically secured and monitored?

Risk Assessment (RA): Are you formally evaluating and tracking risks on a regular basis, and scanning for vulnerabilities on a defined schedule?

Security Assessment (CA): Are you testing whether your controls actually work, and tracking gaps in a Plan of Action and Milestones (POA&M)?

System and Communications Protection (SC): Are your networks, boundaries, and data in transit properly protected? Encryption, network segmentation, and boundary protection all live here.

System and Information Integrity (SI): Are you scanning for threats, patching vulnerabilities, and monitoring for attacks in real time?

The Real Bottleneck: Understanding, Not Capability

Here's where most organizations get stuck; it's not that they lack the tools or the people. It's that when they read a control like "the confidentiality of CUI at rest is protected," they're not sure whether what they're already doing counts, or what specifically an assessor is looking for.

That ambiguity leads to two expensive mistakes:

1. **Over-engineering.** Buying tools or building processes you don't need because the requirement felt bigger than it was.
2. **Under-doing.** Missing something that was already within reach because it didn't feel like enough, or because no one stopped to document it.

Before You Assess the Controls, Get the Scope Right

One of the biggest factors in CMMC complexity is scope. Not every device, system, employee, or application in your company necessarily needs to be assessed against all 110 requirements. CMMC Level 2 defines different treatment for CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets. Getting those categories and the assessment boundary right before you start can significantly reduce unnecessary work.

The vast majority of CMMC Level 2 controls fall into one of three categories.

Category 1: Write It Down

A significant number of assessment objectives involve documenting decisions, processes, responsibilities, and configurations that may already exist in your environment. In many cases, the assessor isn't looking for new technology. They're looking for evidence that the requirement has been defined, implemented, and is operating as intended.

Do you already have a VPN? Write down that it's your approved remote access method, that split tunneling is disabled, and who authorized it.

Do you already enforce password complexity in your identity provider? Document what the rules are and where they're enforced. They're policy acknowledgments of things you've already built.

Many organizations skip this step because it feels like "just paperwork." But during a CMMC assessment, if you cannot provide sufficient objective evidence that a requirement is implemented, the assessor cannot give you credit for it. Documentation is often part of that evidence, but assessors may also rely on interviews, system configurations, logs, demonstrations, and testing.

Category 2: Configure What You Already Have

Many organizations have enterprise tools (Microsoft 365, Google Workspace, an EDR platform, a SIEM, an MDM) that are fully capable of meeting a control requirement but haven't been configured to enforce it yet.

Some examples in more detail include:

Microsoft Entra ID covers Access Control and Authentication through Conditional Access, RBAC, and phishing-resistant MFA.

Microsoft Intune supports Configuration Management and Media Protection via device compliance baselines and endpoint hardening.

Microsoft Defender addresses System and Information Integrity through endpoint detection, response, and vulnerability management.

Microsoft Purview enables CUI classification, Data Loss Prevention, and audit log retention for Audit & Accountability.

Microsoft Sentinel rounds it out as the SIEM backbone for Incident Response and continuous monitoring.

MFA is available but not required for all users. Screen lock is possible but not enforced via Group Policy or MDM profile. Log retention is set to 30 days when the policies and procedures state it should be 90 days. Audit logging is available but not turned on for the right event types.

These are not procurement problems. They're configuration problems — and configuration problems are almost always faster and cheaper to address than buying something new.

Category 3: Add a Genuine Capability

Some controls do require something you don't currently have. A formal vulnerability scanning program. An incident response plan that has been tested with a tabletop exercise. FIPS-validated encryption for CUI that travels outside your organization via email or file share, and FedRAMP authorized tools, such as Virtru.

These gaps require investment, but they typically represent a smaller share of the total picture than most organizations expect when they first see the full list of 110 controls.

Where Organizations Most Often Have Hidden Coverage

These are the areas that consistently surprise organizations during gap assessments.

Logging and Auditing (AU domain). If you're running Microsoft 365 or Google Workspace, you likely already have robust audit logging capabilities. The question is usually whether they're turned on, configured correctly, and retained long enough — not whether the capability exists.

Access Control (AC domain). Most organizations using an identity provider like Entra ID, Okta, or Google Workspace already have the underlying capability for MFA, conditional access, device compliance checks, and session controls. The gap is usually enforcement, not capability.

Configuration Management (CM domain). If you're managing endpoints through Intune, JAMF, or another MDM, you may already be enforcing security baselines. The gap is usually documentation, having a written baseline that your MDM configuration can be formally validated against.

Media Protection (MP domain). Many of these controls are procedural. Do you have a policy for how drives are disposed of? Do you label removable media? These are low-cost wins that often get overlooked because organizations assume compliance requires technical solutions.

Where You Likely Need to Invest

To be balanced about it, a few domains are harder to claim as already covered:

1. Protecting CUI in Transit and at Rest

SC.L2-3.13.8 requires CUI to be protected during transmission using cryptographic mechanisms, unless an allowed alternative physical safeguard is used. SC.L2-3.13.16 requires the confidentiality of CUI to be protected at rest. When cryptography is used to protect the confidentiality of CUI, SC.L2-3.13.11 requires FIPS-validated cryptography.

2. Incident Response Testing

IR.L2-3.6.3 requires that your incident response capability be tested — not just documented. A plan that has never been exercised does not meet this control.

3. Continuous Monitoring

CA.L2-3.12.3 requires ongoing monitoring between formal assessments. Many organizations treat compliance as an annual event rather than an ongoing program, which leaves a meaningful gap here.

4. Vulnerability Management

RA.L2-3.11.2 requires vulnerability scanning periodically and when new vulnerabilities affecting the organization's systems and applications are identified. Organizations without a formal program will need to build one.

Regarding FedRAMP, if you store, process, or transmit CUI in the cloud, the cloud service provider must meet security requirements "equivalent" to the FedRAMP Moderate baseline. This makes Microsoft Commercial M365 not feasible for any controls related to CUI data. One option to continue using Commercial M365 for business is to link it to FedRAMP approved third-party cloud services providers like Virtru, where all CUI is stored in their cloud environment and not Microsoft.

A Note on Data-Centric Protection

A recurring theme across multiple domains (AC.L2-3.1.3, SC.L2-3.13.8, SC.L2-3.13.11, SC.L2-3.13.16) is the question of what happens to CUI after it leaves your environment. Traditional perimeter security protects data while it's inside your network. But once an email is sent to a subcontractor or a file is shared with a partner or government portal, that protection typically ends.

Data-centric encryption addresses this by protecting the data itself, not just the channel it travels through. With tools like Virtru, CUI is encrypted at the message or file level so that only authorized recipients can open it, access can be revoked after the fact, and every access event is logged regardless of where the data ends up. This directly supports several CMMC Level 2 controls that are otherwise difficult to meet with perimeter security alone; and it's one of the areas where organizations most often discover they have a genuine gap worth closing before an assessment.

The Bottom Line

CMMC Level 2 is a serious compliance framework designed to protect sensitive defense information. There is no shortcut to a complete System Security Plan, a tested incident response capability, or a vulnerability management program that is running.

But real work is not the same as starting from scratch. For many organizations we work with, the path to CMMC Level 2 compliance tends to follow three steps that are far less daunting than building a new security stack from the ground up:

Step 1:

Understand what each control is asking. The official assessment guide language is dense by design. Translating it into plain English (as we have done in the reference above) often reveals that you already know exactly what needs to be done.

Step 2:

Take inventory of what you already have. Most organizations are surprised by how much coverage their existing tools provide when those tools are properly configured and documented. Run a gap assessment against your current environment before assuming you need something new.

Step 3:

Fix gaps in the right order. Documentation and configuration gaps first — these are fast and low-cost. Genuine capability gaps second — these take time and investment. This sequence keeps your compliance effort focused and your spending efficient.

CMMC is not designed to be impossible. It is designed to be thorough. Those are different things and recognizing that distinction is often the first step toward making real progress.

If you have questions or need help, don't be shy to reach out to an experienced CMMC expert, preferably an assessor or someone who's helped an organization through a level 2 assessment.

Complete CMMC Level 2 Control Reference

The following tables cover all 320 assessment objectives across all 14 CMMC Level 2 domains. For each objective, you will find the control number, an example of what the assessor is looking for, a plain-English explanation of what it means, and practical guidance on how to address it.

The examples and recommendations below are intended to explain the assessment objectives in practical terms. They are not prescriptive, do not represent the only acceptable method of implementation, and do not create requirements beyond NIST SP 800-171 Rev. 2, 32 CFR Part 170, or applicable CMMC guidance. An assessor will determine whether sufficient objective evidence demonstrates that each applicable assessment objective is satisfied.

Access Control (AC)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.1	**[a]**	Authorized users are identified	Do you have a clear list of everyone who is allowed to use your systems?	Start with a documented user list - who has accounts, who is approved, and who has been offboarded. IAM platforms and directory services make this scalable and keep it current.
AC.L2-3.1.1	**[b]**	Processes acting on behalf of authorized users are identified	Are automated tasks and background scripts also tracked and approved - not just people?	Map your service accounts, scheduled tasks, and API integrations. These are easy to overlook but assessors will specifically ask for them. Automated discovery tools help surface unknown processes.
AC.L2-3.1.1	**[c]**	Devices (and other systems) authorized to connect to the system are identified	Do you know which specific devices are allowed to connect to your network?	Build a device inventory through MDM, endpoint management, or an asset register. Network Access Control (NAC) can technically enforce which devices are allowed before they ever connect.
AC.L2-3.1.1	**[d]**	System access is limited to authorized users	Is your system actually set up to block people who are not on the approved list?	Your identity provider, SSO platform, or Active Directory needs to be configured so unapproved users simply cannot authenticate. Having the list is not enough if the system does not actually check it.
AC.L2-3.1.1	**[e]**	System access is limited to processes acting on behalf of authorized users	Does your system also block unapproved automated processes from running?	Configure your systems to reject any service account or automated process not on your approved list. Automated discovery tools help you find unknown processes running in your environment.
AC.L2-3.1.1	**[f]**	System access is limited to authorized devices (including other systems)	Are unrecognized devices actually prevented from connecting?	Device certificates, MDM enrollment requirements, or conditional access policies that check device compliance before allowing a connection are the technical answer. Unregistered devices simply cannot authenticate.
AC.L2-3.1.2	**[a]**	The types of transactions and functions that authorized users are permitted to execute are defined	For each type of user, have you spelled out what they are and are not allowed to do - not just that they can log in?	Document role-based permissions in your policies and system configurations. This is mostly a people and process effort before you ever touch a tool.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.2	**[b]**	System access is limited to the defined types of transactions and functions for authorized users	Does your system actually enforce those limits, or can people do more than they are supposed to?	Role-based access control (RBAC) in your systems, application-level permissions, and folder permissions technically enforce the roles you defined. Periodic access reviews catch permission drift over time.
AC.L2-3.1.3	**[a]**	Information flow control policies are defined	Have you written rules for where sensitive data is and is not allowed to travel?	Write a policy that maps where CUI is allowed to travel - internally and externally. Virtru can help enforce and audit CUI sharing once it leaves your organization via email or file share.
AC.L2-3.1.3	**[b]**	Methods and enforcement mechanisms for controlling the flow of CUI are defined	Do you have actual tools or technical controls - not just a policy document - that enforce how data can flow?	DLP tools, encrypted email, secure file sharing, and policy-based access controls are the technical side. A policy alone does not enforce data flow. Virtru gives you per-message control over who can open CUI even after it is sent.
AC.L2-3.1.3	**[c]**	Designated sources and destinations for CUI within the system and between interconnected systems are identified	Do you know exactly where your sensitive data comes from and where it is allowed to end up?	Map CUI data flows in a diagram or inventory - where it is created, stored, and which systems or partners it flows to. This is a documentation and discovery exercise, not a technical one.
AC.L2-3.1.3	**[d]**	Authorizations for controlling the flow of CUI are defined	Have you spelled out who is allowed to move sensitive data and under what conditions?	Define who is authorized to share or move CUI and under what conditions. Document this in your policies and tie it to specific roles or approval processes.
AC.L2-3.1.3	**[e]**	Approved authorizations for controlling the flow of CUI are enforced	Are those data movement rules actively being enforced, or just written on paper?	DLP, encrypted email, CASB, and firewalls actively enforce your defined authorizations. Virtru gives you persistent control - CUI can be revoked or expired even after it has already been shared with someone.
AC.L2-3.1.4	**[a]**	The duties of individuals requiring separation are defined	Have you identified which tasks are too risky for one person to control entirely on their own?	Map your organizational roles and identify where a single person controls both sides of a sensitive transaction. Document the problematic combinations before trying to fix them.
AC.L2-3.1.4	**[b]**	Responsibilities for duties that require separation are assigned to separate individuals	Are those risky tasks actually split across different people?	Restructure roles and job descriptions so flagged duties belong to different individuals. Update your RACI matrix, org charts, and role definitions to reflect the separation.
AC.L2-3.1.4	**[c]**	Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals	Do people handling sensitive tasks only have access to their piece - not the whole process?	RBAC and approval workflows technically enforce separation. Configure systems so no single account can complete a sensitive workflow from start to finish without a second person's action being required.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.5	**[a]**	Privileged accounts are identified	Do you have a full list of all admin and elevated-access accounts in your environment?	Audit your directory and cloud platforms for all admin, root, service, and elevated accounts. This often surfaces forgotten accounts and over-provisioned users. PAM platforms can automate discovery.
AC.L2-3.1.5	**[b]**	Access to privileged accounts is authorized in accordance with the principle of least privilege	Are admin-level privileges only given to people whose job actually requires them?	Review each privileged account against the actual job role and remove excess permissions. Just-in-time admin access grants privileges only when needed and removes them automatically afterward.
AC.L2-3.1.5	**[c]**	Security functions are identified	Have you identified which system capabilities are security-sensitive - like configuring firewalls or managing accounts?	Define in writing which system capabilities count as security functions - firewall configuration, audit log access, account management, etc. This scopes the next step.
AC.L2-3.1.5	**[d]**	Access to security functions is authorized in accordance with the principle of least privilege	Is access to those sensitive capabilities limited to only the people who genuinely need them?	Restrict access to those security functions through RBAC and PAM. Periodic access reviews confirm only the right people retain access over time.
AC.L2-3.1.6	**[a]**	Nonsecurity functions are identified	Have you identified which activities in your systems are everyday, non-admin work?	Define which activities are everyday, non-security work - email, documents, business applications. This establishes the baseline for what a standard user account should be able to do.
AC.L2-3.1.6	**[b]**	Users are required to use non-privileged accounts or roles when accessing nonsecurity functions	When admins do regular tasks, are they required to use a standard account instead of their admin account?	Give admins two accounts - a standard one for everyday tasks and a separate admin account for privileged work. Endpoint policies and PAM enforce that admin accounts are not used for regular browsing or email.
AC.L2-3.1.7	**[a]**	Privileged functions are defined	Have you defined which actions in your systems count as privileged - like changing system configurations or creating accounts?	Document a list of privileged functions in your policy - creating accounts, changing firewall rules, accessing audit logs, modifying system configurations. Be specific so there is no ambiguity about what qualifies.
AC.L2-3.1.7	**[b]**	Non-privileged users are defined	Have you clearly defined who your regular, non-admin users are?	Define who falls into the non-privileged category - typically everyone who does not have a documented need for admin access. This is the large majority of your user population.
AC.L2-3.1.7	**[c]**	Non-privileged users are prevented from executing privileged functions	Are regular users technically blocked from taking admin-level actions?	RBAC and endpoint controls technically prevent regular users from accessing privileged functions. PAM tools add an additional layer by requiring explicit elevation for admin tasks.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.7	**[d]**	The execution of privileged functions is captured in audit logs	Is every use of admin-level access being captured in a log?	Configure your SIEM or endpoint platform to log every use of a privileged account or function. This creates the audit trail that lets you trace what was done and by whom after the fact.
AC.L2-3.1.8	**[a]**	The means of limiting unsuccessful logon attempts is defined	Have you set a rule for how many failed login attempts trigger a lockout or delay?	Define the lockout policy in writing - how many failed attempts, what the lockout duration is, and whether it is a hard lockout or a temporary delay. Put the specific numbers in your security policy.
AC.L2-3.1.8	**[b]**	The defined means of limiting unsuccessful logon attempts is implemented	Is that lockout rule actually turned on and enforced in your systems?	Configure account lockout and throttling in your identity provider or Active Directory. Add MFA so even if lockout is briefly bypassed, there is a second barrier. Monitor for brute-force patterns in your SIEM.
AC.L2-3.1.9	**[a]**	Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category	Have you identified the specific legal and security notices that must be shown to users based on the type of sensitive data you handle?	Work with legal or compliance to identify the required notices for each category of CUI you handle. A generic banner may not be enough - notices may need to be CUI-category specific.
AC.L2-3.1.9	**[b]**	Privacy and security notices are displayed	Are those required notices actually being displayed when users access your systems?	Configure login banners across all your systems - M365, Google Workspace, Windows login screens, VPN portals, and any other access points. Test that banners appear before access is granted, not after.
AC.L2-3.1.10	**[a]**	The period of inactivity after which the system initiates a session lock is defined	Have you defined how long a screen can sit idle before it locks itself?	Define the inactivity period in your security policy - 15 minutes is a common starting point. Document it clearly so configurations can be validated against the policy during an assessment.
AC.L2-3.1.10	**[b]**	Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity	Does the screen actually lock after that idle period - blocking access to what was open?	Configure screen lock timeouts through Group Policy, MDM, or endpoint management. Verify the setting is applied and cannot be overridden by users on their own.
AC.L2-3.1.10	**[c]**	Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity	When the screen locks, does it fully hide what was on screen, or just freeze the image?	Configure the lock screen to display a blank screen or screensaver - not a frozen image of what was open. Most OS-level screen lock settings handle this by default, but verify it is actually working.
AC.L2-3.1.11	**[a]**	Conditions requiring a user session to terminate are defined	Have you defined what triggers a session to automatically end - like a timeout or inactivity?	Define session termination conditions in your policy - maximum session length, inactivity threshold, or logout on VPN disconnect. Be specific enough that these can actually be configured in your systems.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.11	**[b]**	A user session is automatically terminated after any of the defined conditions occur	Do sessions actually end on their own when those conditions are met?	Configure session timeout settings in your applications, VPN, and cloud platforms. Conditional access policies can enforce maximum token lifetimes to ensure sessions do not persist indefinitely.
AC.L2-3.1.12	**[a]**	Remote access sessions are permitted	Have you approved which methods employees are allowed to use to access your systems remotely?	Create a written policy that formally approves which remote access methods are permitted. Whatever is in use - VPN, ZTNA, remote desktop - should be explicitly approved in writing, not just assumed to be fine.
AC.L2-3.1.12	**[b]**	The types of permitted remote access are identified	Have you specifically documented which remote access types are permitted?	List the specific approved remote access types in your policy and documentation - not just that remote access is allowed, but the actual named methods and tools in use.
AC.L2-3.1.12	**[c]**	Remote access sessions are controlled	Is remote access actively managed and controlled - not just left open once it is set up?	Enforce controls on remote sessions - MFA at login, device compliance checks, session recording where appropriate. ZTNA provides more granular control than traditional VPN by limiting access to specific resources.
AC.L2-3.1.12	**[d]**	Remote access sessions are monitored	Are remote connections being watched and logged?	Log all remote sessions - who connected, from where, at what time, and for how long. SIEM correlation can flag unusual patterns like off-hours connections or access from unexpected locations.
AC.L2-3.1.13	**[a]**	Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified	Have you identified what encryption is being used to protect your remote connections?	Document which encryption protocols protect your remote connections - TLS version, cipher suites, VPN protocol. This should go into your SSP and be specific enough to validate technically.
AC.L2-3.1.13	**[b]**	Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented	Is that encryption actually in place and working?	Configure your VPN or remote access solution to use FIPS-validated encryption. Collect configuration screenshots or exported settings as evidence that the right protocols are in use and weaker ones are disabled.
AC.L2-3.1.14	**[a]**	Managed access control points are identified and implemented	Have you identified the approved gateways or entry points that all remote connections must go through?	Identify and document the specific gateways, VPN concentrators, or ZTNA access points that all remote connections must pass through. Include them in your network diagrams.
AC.L2-3.1.14	**[b]**	Remote access is routed through managed network access control points	Are all remote connections actually routing through those approved paths - no shortcuts around them?	Configure your network so remote devices cannot bypass the approved gateways. Firewall rules and routing configurations enforce this. Test to confirm there are no alternate paths around your managed access points.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.15	**[a]**	Privileged commands authorized for remote execution are identified	Have you listed which admin commands can actually be run from a remote location?	Write a list of which privileged commands are authorized for remote execution. Anything not on the list is not permitted remotely. PAM jump servers and session recording add the technical enforcement.
AC.L2-3.1.15	**[b]**	Security-relevant information authorized to be accessed remotely is identified	Have you listed which sensitive information is allowed to be accessed remotely?	Document which types of security-relevant information are permitted to be accessed from a remote location, and under what conditions. This should be a short, specific list.
AC.L2-3.1.15	**[c]**	The execution of the identified privileged commands via remote access is authorized	Is running those admin commands remotely formally authorized - not just assumed to be fine?	Require formal authorization - documented approval from a manager or ISSO - for each type of remote privileged command before it is permitted. PAM tools can enforce this technically.
AC.L2-3.1.15	**[d]**	Access to the identified security-relevant information via remote access is authorized	Is accessing that sensitive information remotely formally authorized?	Require formal authorization for remote access to security-relevant information as well. Document approvals and configure PAM or RBAC to enforce access limitations.
AC.L2-3.1.16	**[a]**	Wireless access points are identified	Do you have a complete inventory of every Wi-Fi access point in your environment?	Walk the facility and document every wireless access point, including any personal hotspots or shadow IT access points. Wireless scanning tools can detect rogue APs you might have missed during a manual walkthrough.
AC.L2-3.1.16	**[b]**	Wireless access is authorized prior to allowing such connections	Must devices be approved before they are allowed to connect over Wi-Fi?	Require device certificates or NAC enrollment before wireless access is granted. A shared pre-shared key does not meet authorization requirements - devices should be individually approved before connecting.
AC.L2-3.1.17	**[a]**	Wireless access to the system is protected using authentication	Does your wireless network require proper authentication - not just a shared password anyone can use?	Configure WPA2 or WPA3 Enterprise with RADIUS authentication on all corporate wireless networks. This ensures each device authenticates individually rather than sharing a common network password.
AC.L2-3.1.17	**[b]**	Wireless access to the system is protected using encryption	Is data encrypted while traveling over your wireless network?	WPA2/WPA3 Enterprise encrypts wireless traffic in transit. For CUI transmitted over Wi-Fi, adding application-layer encryption like TLS or Virtru ensures data is protected even if the wireless layer is somehow compromised.
AC.L2-3.1.18	**[a]**	Mobile devices that process, store, or transmit CUI are identified	Have you identified all phones, tablets, and laptops that handle sensitive data?	Build a mobile device inventory through your MDM or UEM platform. Include phones, tablets, and laptops that access CUI - even personal devices used for work email may be in scope depending on your environment.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.18	**[b]**	Mobile device connections are authorized	Do mobile devices need to be approved before connecting to your systems?	Require MDM enrollment and a compliance check before mobile devices are allowed to connect. Conditional access policies can automatically block non-compliant or unenrolled devices.
AC.L2-3.1.18	**[c]**	Mobile device connections are monitored and logged	Are mobile device connections being tracked and logged?	MDM platforms log device connections, compliance status, and access events. Feed this data into your SIEM or review it on a defined schedule to maintain ongoing visibility.
AC.L2-3.1.19	**[a]**	Mobile devices that process, store, or transmit CUI are identified for encryption purposes	Have you identified every mobile device that stores or processes sensitive data?	Your MDM inventory from the previous control is a good starting point. Flag every device in that inventory that specifically touches CUI - through email, file access, or applications.
AC.L2-3.1.19	**[b]**	Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms	If a mobile device was lost or stolen, would the sensitive data on it be unreadable?	Enable full-disk encryption or container encryption on all identified mobile devices. MDM platforms can enforce this as a compliance requirement and flag devices that do not meet the standard.
AC.L2-3.1.20	**[a]**	Connections to external systems are identified	Have you identified all external systems and cloud services your organization connects to?	Document every external system your organization connects to - cloud platforms, government portals, partner systems, third-party vendors. Network diagrams and a system interconnection inventory make this manageable.
AC.L2-3.1.20	**[b]**	The use of external systems is identified	Do you know which external services your employees are actually using day to day?	Survey employees and IT to understand which external services are actually being used day to day. CASB tools can discover shadow IT usage automatically and may surface services you did not know about.
AC.L2-3.1.20	**[c]**	Connections to external systems are verified	Have those external connections been verified as legitimate and appropriately secured?	Conduct vendor due diligence on each identified external connection - review their security posture, agreements, and access controls. Document the verification so you can show the assessor you checked.
AC.L2-3.1.20	**[d]**	The use of external systems is verified	Have the external services employees use been confirmed as approved and appropriate?	Review and confirm that external services employees are using are on the approved list and have been properly evaluated. CASB tools can flag unapproved service usage in real time.
AC.L2-3.1.20	**[e]**	Connections to external systems are controlled/limited	Are connections to external systems actively limited - not open-ended?	Enforce allowlists through firewall rules, CASB policies, and conditional access to limit which external systems can be connected to. Virtru helps protect CUI that does flow to approved external partners by encrypting it at the file or message level.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AC.L2-3.1.20	**[f]**	The use of external systems is controlled/limited	Is employee use of external systems being managed - not access to just anything they choose?	CASB tools and DLP policies enforce limits on how approved external systems are used - blocking uploads of CUI to unauthorized areas even within a generally approved service.
AC.L2-3.1.21	**[a]**	The use of portable storage devices containing CUI on external systems is identified and documented	Have you documented when and how portable drives with sensitive data get used on external systems?	Document every instance of portable drives with CUI being used on external systems - who did it, when, what was on the drive, and which external system it connected to. Make this a standard part of your media tracking process.
AC.L2-3.1.21	**[b]**	Limits on the use of portable storage devices containing CUI on external systems are defined	Have you set rules limiting when that is actually permitted?	Write a policy defining the rules - when is it permitted, who must approve it, what encryption is required. Be specific enough that someone can follow the policy without having to interpret it.
AC.L2-3.1.21	**[c]**	The use of portable storage devices containing CUI on external systems is limited as defined	Are those portable media rules being followed in practice?	Endpoint device control tools can technically restrict which USB devices can connect to which systems. Combine this with the approval and logging process defined in your policy.
AC.L2-3.1.22	**[a]**	Individuals authorized to post or process information on publicly accessible systems are identified	Have you defined who is allowed to post content on your public-facing websites or portals?	Maintain a documented list of who has permission to post or manage content on your public websites, portals, or social platforms. Keep this list small and review it regularly.
AC.L2-3.1.22	**[b]**	Procedures to ensure CUI is not posted or processed on publicly accessible systems are identified	Do you have a documented process to ensure sensitive data never ends up posted publicly?	Write a procedure specifically addressing CUI - what constitutes CUI, how to confirm something is not CUI before posting, and who approves public content. Post it somewhere content creators will actually see it.
AC.L2-3.1.22	**[c]**	A review process is in place prior to posting of any content to publicly accessible systems	Does anything going public go through a review before it is posted?	Require content to pass through a review and approval workflow before it goes live. Even a simple documented email approval chain is better than no process at all.
AC.L2-3.1.22	**[d]**	Content on publicly accessible systems is reviewed to ensure that it does not include CUI	Is existing public content periodically checked to confirm nothing sensitive slipped through?	Schedule periodic reviews of existing public content - quarterly is reasonable. DLP scanning tools can help automate detection of potentially sensitive content already posted.
AC.L2-3.1.22	**[e]**	Mechanisms are in place to remove and address improper posting of CUI	If sensitive data was accidentally posted publicly, do you have a process to quickly remove it and address it?	Define a takedown procedure - who has authority to remove content, how quickly it must happen, and who gets notified. Test it before you need it so the team knows what to do under pressure.

Awareness and Training (AT)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AT.L2-3.2.1	**[a]**	Security risks associated with organizational activities involving CUI are identified	Have you identified the specific security risks that come with your employees handling sensitive data?	Conduct a review of your CUI-handling activities and document the specific security risks associated with each. Focus on where CUI is created, stored, and shared - not every possible risk in the organization.
AT.L2-3.2.1	**[b]**	Policies, standards, and procedures related to the security of the system are identified	Are your security policies and procedures written down somewhere people can actually find and reference them?	Compile your security policies, standards, and procedures in a central location employees can actually access. Assessors want to see that these exist and are findable - not just that someone says they have them.
AT.L2-3.2.1	**[c]**	Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities	Do your managers, IT staff, and regular users actually know the risks tied to their specific work?	Deliver security awareness training to all staff at least annually. An LMS platform makes delivery and tracking easy. Phishing simulations demonstrate ongoing reinforcement beyond a once-a-year click-through.
AT.L2-3.2.1	**[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	Do those same people know the actual rules and policies that apply to their role?	Ensure training content includes the specific policies and procedures relevant to each audience. Managers, admins, and regular users may each need tailored content - not the same generic security module.
AT.L2-3.2.2	**[a]**	Information security-related duties, roles, and responsibilities are defined	Has each person's security responsibility been clearly defined?	Document security responsibilities in job descriptions, role charters, or a RACI matrix. Every person with a security duty should have it formalized in writing - not just assumed as part of their job.
AT.L2-3.2.2	**[b]**	Information security-related duties, roles, and responsibilities are assigned to designated personnel	Are those security responsibilities formally assigned to specific individuals - not just assumed someone will handle it?	Formally assign security duties to named individuals, not just roles. This creates accountability and makes it clear who the assessor should be talking to about specific controls.
AT.L2-3.2.2	**[c]**	Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities	Have people with assigned security duties been trained on what they are responsible for?	Provide role-specific training to people with assigned security duties - IR training for the IR team, admin training for admins, etc. Keep completion records as evidence of compliance.
AT.L2-3.2.3	**[a]**	Potential indicators associated with insider threats are identified	Have you identified the warning signs that a trusted insider might be becoming a security risk?	Document behavioral and technical indicators of insider threats - unusual data access patterns, bulk downloads, sudden behavioral changes. Reference established frameworks like CERT's insider threat indicators as a starting point.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AT.L2-3.2.3	[b]	Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees	Have managers and employees been trained to recognize those warning signs and know how to report them?	Incorporate insider threat awareness into your annual security training. Include how to report concerns through HR or a dedicated confidential reporting channel. A clear, low-friction reporting path increases early detection.

Audit and Accountability (AU)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AU.L2-3.3.1	[a]	Audit logs needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified	Have you decided which types of events your systems need to log - like logins, file access, or admin actions?	Define in a written policy which event types need to be logged - logins, failed logins, privilege use, file access, configuration changes. Tie these to the activities that would indicate unauthorized or unlawful behavior.
AU.L2-3.3.1	[b]	The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined	Have you defined what information each log entry must include - timestamp, who did it, what they did?	Define the required fields for each log entry - timestamp, user ID, action performed, result, source IP, affected resource. This becomes your audit record standard that all systems must match.
AU.L2-3.3.1	[c]	Audit records are created (generated)	Are your systems actually generating those log records - not just capable of doing so?	Configure your endpoints, servers, cloud platforms, and network devices to actually generate logs. Verify logging is enabled - it is often misconfigured or turned off by default in some systems.
AU.L2-3.3.1	[d]	Audit records, once created, contain the defined content	Do the logs actually being produced include all the required fields?	Pull sample logs and compare them to your defined standard. Gaps in log content - missing user IDs, timestamps without source context - are a common assessor finding that is easy to miss until someone actually looks.
AU.L2-3.3.1	[e]	Retention requirements for audit records are defined	Have you set a rule for how long logs must be kept?	Define your log retention period in policy - 90 days online and 1-3 years archived is a common and defensible approach. Match your retention policy to your contractual requirements, which may specify minimums.
AU.L2-3.3.1	[f]	Audit records are retained as defined	Are logs actually being retained for that required period?	Configure your log storage and SIEM with retention rules that match your policy. Set up automated archiving before logs age out of active storage. Test restoration from archive periodically to confirm it works.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AU.L2-3.3.2	**[a]**	The content of the audit records needed to support the ability to uniquely trace users to their actions is defined	Have you defined what a log needs to contain to trace any action back to the specific person who did it?	Define what your audit records must contain to trace actions to individuals - at minimum, a unique user ID, timestamp, action performed, and the affected object or resource. Write this into your logging policy.
AU.L2-3.3.2	**[b]**	Audit records, once created, contain the defined content	Do your actual logs include that level of detail - individual user IDs, session info, timestamps?	Eliminate shared accounts and audit your current logs to confirm user IDs - not just IP addresses or device names - are present in all entries. SIEM correlation rules can flag log sources missing this detail.
AU.L2-3.3.3	**[a]**	A process for determining when to review logged events is defined	Do you have a process for periodically reviewing whether you are logging the right types of events?	Define a review schedule in your policy - at least annually, or after significant system changes. Build this review into your security program calendar so it actually happens.
AU.L2-3.3.3	**[b]**	Event types being logged are reviewed in accordance with the defined review process	Is that review actually happening on schedule?	Execute the review on schedule. Pull your current log source list, compare it to your event type requirements, and confirm coverage across all in-scope systems.
AU.L2-3.3.3	**[c]**	Event types being logged are updated based on the review	When the review finds gaps, are changes actually made to what is being logged?	When the review reveals gaps, update configurations and document the change. A record of what was corrected and when shows the process is actually working and not just theoretical.
AU.L2-3.3.4	**[a]**	Personnel or roles to be alerted in the event of an audit logging process failure are identified	Have you designated who gets notified if your logging system breaks down or stops working?	Designate specific individuals or roles to receive alerts when logging fails. Put this in writing - who is responsible for responding to a logging system outage, and what the response should look like.
AU.L2-3.3.4	**[b]**	Types of audit logging process failures for which alert will be generated are defined	Have you defined what kinds of logging failures trigger that alert?	Define what failure conditions trigger an alert - agent going offline, storage reaching capacity, events being dropped, log forwarding stopping. The more specific the definition, the easier it is to configure alerting.
AU.L2-3.3.4	**[c]**	Identified personnel or roles are alerted in the event of an audit logging process failure	When a logging failure happens, do the right people actually get notified?	Configure your SIEM or log management platform to generate alerts for those failure conditions and route them to the designated people. Test the alerting to confirm it actually fires when it should.
AU.L2-3.3.5	**[a]**	Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined	Do you have a defined process for reviewing logs to find suspicious or unusual activity?	Document a log review and analysis process - how often logs are reviewed, who does the review, what suspicious patterns trigger escalation, and how findings are handled and tracked.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AU.L2-3.3.5	**[b]**	Defined audit record review, analysis, and reporting processes are correlated	Are logs from multiple systems being combined so you can spot patterns across your environment?	Feed logs from all your systems into a central SIEM where correlation rules can connect events across endpoints, network, cloud, and applications. Cross-system correlation is how sophisticated attacks get caught.
AU.L2-3.3.6	**[a]**	An audit record reduction capability that supports on-demand analysis is provided	Do you have a way to filter down large volumes of log data to find what actually matters?	Your SIEM should let analysts filter large log volumes down to the events that matter. Make sure query and search capabilities are being actively used - not just collecting data in the background.
AU.L2-3.3.6	**[b]**	A report generation capability that supports on-demand reporting is provided	Can you generate reports from your log data on demand when needed?	Configure scheduled reports and on-demand reporting in your SIEM. Test that you can generate an investigation-ready report on demand before you are under pressure to produce one during an incident.
AU.L2-3.3.7	**[a]**	Internal system clocks are used to generate time stamps for audit records	Do your systems use their own internal clock to timestamp log entries?	Verify that all systems use their internal clock for log timestamps. This is typically the default but can be changed - confirm it in your system configurations, especially in virtual environments.
AU.L2-3.3.7	**[b]**	An authoritative source with which to compare and synchronize internal system clocks is specified	Have you designated a trusted time source that all systems sync their clocks to?	Designate an authoritative time source - an NTP pool server or a time service from NIST or your cloud provider. Document it in your configuration standards so all systems know where to sync.
AU.L2-3.3.7	**[c]**	Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source	Are all your system clocks actually syncing to that authoritative source so timestamps line up across systems?	Configure all systems to sync to your designated NTP source and verify clock sync is working. In cloud environments, most platforms handle this automatically - document the service being used as evidence.
AU.L2-3.3.8	**[a]**	Audit information is protected from unauthorized access	Are your audit logs protected so only authorized people can read them?	Configure RBAC on your SIEM and log storage so only designated logging administrators can access raw logs. Regular analysts should have read access limited to what they need for their role.
AU.L2-3.3.8	**[b]**	Audit information is protected from unauthorized modification	Are your logs protected from being changed or tampered with?	Use immutable log storage or write-once configurations to prevent tampering. At minimum, ensure only a small group can modify log configurations, and that any modifications are themselves logged and alerted on.
AU.L2-3.3.8	**[c]**	Audit information is protected from unauthorized deletion	Are your logs protected from being deleted?	Immutable storage and retention locks prevent deletion. Configure deletion restrictions so even logging admins cannot delete logs without a formal secondary approval process.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
AU.L2-3.3.8	**[d]**	Audit logging tools are protected from unauthorized access	Are the tools that collect and manage logs protected from unauthorized access?	Apply RBAC to your log collection agents, SIEM platform, and forwarding infrastructure. Only logging administrators should be able to access the tools themselves - not just the logs they produce.
AU.L2-3.3.8	**[e]**	Audit logging tools are protected from unauthorized modification	Are those logging tools protected from being modified or tampered with?	Configure change controls on your logging tool settings. Any modification to log sources, forwarding rules, or collection configurations should require authorized approval and trigger an alert.
AU.L2-3.3.8	**[f]**	Audit logging tools are protected from unauthorized deletion	Are those logging tools protected from being removed or destroyed?	Protect logging infrastructure physically as well - treat logging servers and agents as critical infrastructure subject to the same physical access controls and backup procedures as your most sensitive systems.
AU.L2-3.3.9	**[a]**	A subset of privileged users granted access to manage audit logging functionality is defined	Have you designated a small, specific group of people allowed to manage the audit logging system?	Define a small, named group of logging administrators in your policy and system configurations. Separate this from general IT or security roles - not everyone on the security team should have logging admin access.
AU.L2-3.3.9	**[b]**	Management of audit logging functionality is limited to the defined subset of privileged users	Is access to manage or configure logging restricted strictly to that group?	Configure your SIEM and log management platform so only that defined group can make administrative changes - adding log sources, changing retention, modifying alert rules. Test it to confirm others are actually blocked.

Configuration Management (CM)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CM.L2-3.4.1	**[a]**	A baseline configuration is established	Have you created a documented standard configuration that all your systems should match?	Create a documented standard configuration for your system types - servers, workstations, cloud instances, network devices. Configuration management tools, CMDB platforms, or even structured templates can help build and maintain this.
CM.L2-3.4.1	**[b]**	The baseline configuration includes hardware, software, firmware, and documentation	Does that baseline cover hardware, software, firmware, and documentation - not just one layer?	Ensure your baseline covers all layers - OS settings, installed software versions, firmware, and relevant documentation like network diagrams and data flow maps. A baseline limited to one layer will have gaps.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CM.L2-3.4.1	**[c]**	The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle	Is the baseline kept current as systems evolve - not just created once and never updated?	Treat the baseline as a living document. Update it when new system types are deployed, when patching changes configurations, or when security settings are modified. Version control helps track changes over time.
CM.L2-3.4.1	**[d]**	A system inventory is established	Do you have an active inventory of all the systems in your environment?	Build and maintain an asset inventory covering all in-scope systems. Asset management tools, MDM platforms, and network scanners can automate discovery and reduce the risk of missing something.
CM.L2-3.4.1	**[e]**	The system inventory includes hardware, software, firmware, and documentation	Does that inventory cover hardware, software, firmware, and documentation?	Make sure your inventory goes beyond just hostnames and IP addresses - include hardware models, software and firmware versions, and associated documentation.
CM.L2-3.4.1	**[f]**	The inventory is maintained (reviewed and updated) throughout the system development life cycle	Is the inventory actively updated when things are added, removed, or changed?	Update the inventory when assets are added, changed, or decommissioned. Automated discovery tools reduce stale entries. Schedule periodic reviews to catch anything that slipped through manual processes.
CM.L2-3.4.2	**[a]**	Security configuration settings for information technology products employed in the system are established and included in the baseline configuration	Have you defined the specific security settings that every device and system should be configured to?	Start with CIS Benchmarks or STIGs as a baseline for your security configuration settings. Adapt them to your environment and document any accepted deviations with a rationale and formal approval.
CM.L2-3.4.2	**[b]**	Security configuration settings for information technology products employed in the system are enforced	Are those secure settings actually applied in practice - not just listed in a document?	Apply the defined configurations through Group Policy, MDM profiles, cloud security policies, or configuration management tools. Monitor for configuration drift - settings can revert after patching or system changes.
CM.L2-3.4.3	**[a]**	Changes to the system are tracked	Is every change to your systems being tracked with a record of what changed, when, and by whom?	Every system change should generate a record - what changed, on which system, by whom, and when. ITSM platforms or structured ticketing workflows satisfy this without needing complex tooling.
CM.L2-3.4.3	**[b]**	Changes to the system are reviewed	Do proposed changes go through a review before they are made?	Build a review step into your change process so changes are evaluated before they move forward - not just submitted and executed. Someone other than the requestor should review the proposed change.
CM.L2-3.4.3	**[c]**	Changes to the system are approved or disapproved	Do changes require formal approval before going through?	Assign clear approval authority to a specific person or change board. Unapproved changes should not be implemented, and rejected changes should be documented with the reason.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CM.L2-3.4.3	**[d]**	Changes to the system are logged	Is there a log of all approved and rejected changes?	Your change management system should automatically log approved and rejected changes. This log becomes the audit trail showing that changes were controlled and not just made ad hoc.
CM.L2-3.4.4	**[a]**	The security impact of changes to the system is analyzed prior to implementation	Before making a change to a system, do you assess whether it could introduce new security risks?	Add a security impact question to every change request - does this change affect CUI handling, access controls, or system exposure? Require a security team signoff for anything that could affect your security posture.
CM.L2-3.4.5	**[a]**	Physical access restrictions associated with changes to the system are defined	Have you defined who is physically permitted to access systems or hardware in order to make changes?	Define in writing who is physically allowed to touch hardware or equipment to make changes. Tie this to your physical access control list so it is enforceable, not just advisory.
CM.L2-3.4.5	**[b]**	Physical access restrictions associated with changes to the system are documented	Are those physical access restrictions written down?	Document those physical access restrictions in your change management or physical security policy. Named roles or named individuals are clearer than vague descriptions.
CM.L2-3.4.5	**[c]**	Physical access restrictions associated with changes to the system are approved	Have those physical restrictions been formally approved?	Get formal approval for the physical access list from a manager or ISSO. Document the approval date and reviewer name so the authorization chain is clear.
CM.L2-3.4.5	**[d]**	Physical access restrictions associated with changes to the system are enforced	Are those physical restrictions actually enforced in practice?	Enforce physical restrictions through badge access controls, locked equipment cages, and escort requirements. Badge access logs provide the ongoing evidence that controls are working in practice.
CM.L2-3.4.5	**[e]**	Logical access restrictions associated with changes to the system are defined	Have you defined who is allowed to make changes through admin or network access?	Define who has the admin credentials or elevated access needed to make logical changes - not just physical access to the hardware, but software-level changes through admin accounts or remote management tools.
CM.L2-3.4.5	**[f]**	Logical access restrictions associated with changes to the system are documented	Are those logical access restrictions documented?	Document the logical access restrictions in your change management policy - which roles can make what types of changes, and through which systems.
CM.L2-3.4.5	**[g]**	Logical access restrictions associated with changes to the system are approved	Have those logical restrictions been formally approved?	Get formal approval for logical access assignments from a manager or ISSO. Document it the same way as physical access approvals so both are captured.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CM.L2-3.4.5	**[h]**	Logical access restrictions associated with changes to the system are enforced	Are those logical access restrictions for changes actually enforced?	Enforce logical access restrictions through RBAC and PAM. Only approved accounts should have the permissions needed to implement changes. Review these permissions regularly to prevent accumulation over time.
CM.L2-3.4.6	**[a]**	Essential system capabilities are defined based on the principle of least functionality	Have you defined only the capabilities each system actually needs to do its job?	For each system, define only the capabilities it needs to fulfill its business purpose. A server running only a web application does not need a database engine, print services, or Bluetooth enabled.
CM.L2-3.4.6	**[b]**	The system is configured to provide only the defined essential capabilities	Are systems configured to run only those required capabilities – with everything else turned off?	Configure systems to run only those defined essential capabilities. Disable unnecessary Windows services, remove unused software, and lock down network-facing features. CIS Benchmarks are a practical starting point.
CM.L2-3.4.7	**[a]**	Essential programs are defined	Have you identified which programs are essential to your operations?	Build a list of essential programs required for each system type. This becomes your software allowlist baseline and informs your application execution policy.
CM.L2-3.4.7	**[b]**	The use of nonessential programs is defined	Have you defined what programs are nonessential and what the rules are for them?	For programs that are not essential, define whether they are prohibited entirely or permitted with restrictions. Document the rationale for anything you choose to allow with conditions rather than blocking outright.
CM.L2-3.4.7	**[c]**	The use of nonessential programs is restricted, disabled, or prevented as defined	Are nonessential programs restricted, disabled, or prevented from running?	Use application control, EDR, or endpoint management to prevent nonessential programs from running. Allowlisting is the strongest approach – only approved software executes, everything else is blocked.
CM.L2-3.4.7	**[d]**	Essential functions are defined	Have you identified which system functions are essential to your business?	Define which system functions are essential to your operations – like remote management tools, scripting engines, or database services that are actively used.
CM.L2-3.4.7	**[e]**	The use of nonessential functions is defined	Have you defined which functions are nonessential?	For functions that are not essential, decide whether to disable them entirely or restrict them with compensating controls. Document the decision and the rationale.
CM.L2-3.4.7	**[f]**	The use of nonessential functions is restricted, disabled, or prevented as defined	Are nonessential functions turned off or blocked?	Apply the restrictions in your system configurations. Endpoint management and hardening scripts can disable nonessential functions at scale across your fleet.
CM.L2-3.4.7	**[g]**	Essential ports are defined	Have you identified which network ports need to be open to support your work?	Run a port scan against your systems to see what is actually open and listening. Document which ports need to be open for legitimate business operations.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CM.L2-3.4.7	**[h]**	The use of nonessential ports is defined	Have you defined which ports are nonessential and should not be open?	Identify all ports that are open but not needed for business operations. These become candidates for closure in your firewall and host-based security configurations.
CM.L2-3.4.7	**[i]**	The use of nonessential ports is restricted, disabled, or prevented as defined	Are nonessential network ports closed or blocked?	Configure your firewall and host-based controls to close or block nonessential ports. Rerun port scans after changes to verify closure and catch any that were missed.
CM.L2-3.4.7	**[j]**	Essential protocols are defined	Have you identified which network protocols are required for your operations?	Document which network protocols are needed for your operations - HTTPS, DNS, SMTP, etc. This forms your protocol allowlist.
CM.L2-3.4.7	**[k]**	The use of nonessential protocols is defined	Have you defined which protocols are nonessential?	Identify protocols that are not needed - like Telnet, FTP, or deprecated SSL/TLS versions. These are the targets for restriction or disablement.
CM.L2-3.4.7	**[l]**	The use of nonessential protocols is restricted, disabled, or prevented as defined	Are nonessential protocols restricted or disabled?	Disable or restrict nonessential protocols through firewall rules, switch configurations, and application settings. Verify the restrictions are in place through testing or scanning.
CM.L2-3.4.7	**[m]**	Essential services are defined	Have you identified which services need to be running on your systems?	Identify which services need to be running on each system type to support actual business operations - not just services that came installed with the OS.
CM.L2-3.4.7	**[n]**	The use of nonessential services is defined	Have you defined which services are nonessential?	Identify services that are running but not needed - often enabled by default during OS installation. These are unnecessary attack surface and should be addressed.
CM.L2-3.4.7	**[o]**	The use of nonessential services is restricted, disabled, or prevented as defined	Are nonessential services stopped and prevented from running?	Stop and disable nonessential services through system hardening scripts or configuration management tools. Verify the changes persist after reboots.
CM.L2-3.4.8	**[a]**	A policy specifying whether whitelisting or blacklisting is to be implemented is specified	Have you decided whether you are using an allowlist or a blocklist approach to control what software runs?	Document your software execution approach in policy - whether you are using allowlisting, denylisting, or a combination. Justify the choice based on your environment and the risk level you are managing.
CM.L2-3.4.8	**[b]**	The software allowed to execute under whitelisting or denied use under blacklisting is specified	Have you documented which software is specifically allowed or denied under your chosen approach?	Maintain a documented list of approved software for allowlisting, or prohibited software for denylisting. Keep it current - the list has no value if it does not reflect what is actually in your environment.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CM.L2-3.4.8	**[c]**	Whitelisting or blacklisting is implemented as specified	Is that allowlist or blocklist approach actually implemented and functioning in your systems?	Implement the policy through application control tools, EDR, or OS features like AppLocker or Windows Defender Application Control. Test to confirm only the intended software can actually execute.
CM.L2-3.4.9	**[a]**	A policy for controlling the installation of software by users is established	Do you have a written policy defining what software users are allowed to install on their own?	Write a policy defining what users can and cannot install on their own. Be specific – some organizations allow approved business software, others require IT approval for everything without exception.
CM.L2-3.4.9	**[b]**	Installation of software by users is controlled based on the established policy	Is software installation by users actually controlled based on that policy?	Remove local administrator rights from standard user accounts. Without admin rights, users cannot install most software without IT involvement. A software distribution platform gives users a safe, approved channel for requests.
CM.L2-3.4.9	**[c]**	Installation of software by users is monitored	Are you monitoring what software gets installed on your systems?	Use EDR, MDM, or application control tools to alert when software is installed on your systems. Even if a user finds a workaround, monitoring catches it quickly and creates a record.

Identification and Authentication (IA)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IA.L2-3.5.1	**[a]**	System users are identified	Does every user have a unique identity in your systems - no shared or anonymous accounts?	Build or audit your user directory so every user has a unique account tied to a real, identified person. Remove or disable any generic, shared, or anonymous accounts you find.
IA.L2-3.5.1	**[b]**	Processes acting on behalf of users are identified	Do automated processes also have their own defined identity - not running under a generic account?	Inventory all service accounts, API integrations, scheduled tasks, and automation scripts. Assign each a unique identity with a documented owner. Generic accounts with no clear owner need to be formalized or eliminated.
IA.L2-3.5.1	**[c]**	Devices accessing the system are identified	Does every device that connects to your systems have its own recognized identity?	Build or audit your device inventory - MAC addresses, certificates, or MDM enrollment can all establish unique device identities. NAC systems tie device authentication to that inventory at the network layer.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IA.L2-3.5.2	**[a]**	The identity of each user is authenticated or verified as a prerequisite to system access	Is every user required to prove who they are before they can access your systems?	Configure your identity provider to require authentication before users can access any system. Remove default credentials, enforce password requirements, and extend this to applications and cloud platforms, not just workstation login.
IA.L2-3.5.2	**[b]**	The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access	Are automated processes also required to authenticate before getting access?	Ensure automated processes and service accounts also authenticate before accessing resources. Use managed service accounts, certificates, or API keys - not hard-coded credentials buried in scripts.
IA.L2-3.5.2	**[c]**	The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access	Are devices required to authenticate before they are allowed to connect?	Require device authentication before network access is granted. Device certificates, MDM enrollment checks, and 802.1X-based NAC accomplish this at the network layer without requiring user action.
IA.L2-3.5.3	**[a]**	Privileged accounts are identified	Have you identified all admin and elevated-privilege accounts that need MFA?	Run an audit of your accounts to identify all privileged accounts across your environment. This list becomes the scope for your MFA enforcement effort - you cannot enforce MFA where you do not know accounts exist.
IA.L2-3.5.3	**[b]**	Multifactor authentication is implemented for local access to privileged accounts	Do admin accounts require more than just a password when logging in locally?	Configure MFA through your identity provider for local admin logins. Hardware keys or authenticator apps are both valid approaches. A password alone does not meet this requirement regardless of complexity.
IA.L2-3.5.3	**[c]**	Multifactor authentication is implemented for network access to privileged accounts	Do admin accounts require more than just a password when logging in over the network?	Enforce MFA for all network-based logins to privileged accounts. Conditional access policies can block network access if MFA is not satisfied, regardless of whether the password is correct.
IA.L2-3.5.3	**[d]**	Multifactor authentication is implemented for network access to non-privileged accounts	Do regular user accounts also require more than just a password for network access?	Extend MFA to all user accounts for network access - not just admins. Conditional access policies in most identity platforms allow broad enforcement with minimal friction through authenticator apps.
IA.L2-3.5.4	**[a]**	Replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts	Does your authentication method prevent attackers from reusing a captured login credential to break in later?	MFA inherently addresses replay resistance for most authentication scenarios. Additionally, ensure you are using modern protocols like Kerberos or SAML, and have disabled any legacy protocols that allow credential replay.
IA.L2-3.5.5	**[a]**	A period within which identifiers cannot be reused is defined	Have you set a rule for how long a username or device ID must sit unused before it can be reassigned to someone new?	Define a waiting period - commonly 90 to 180 days - before a retired username or device ID can be reassigned. Put this in your account management policy with enough specificity to be enforceable.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IA.L2-3.5.5	**[b]**	Reuse of identifiers is prevented within the defined period	Is that waiting period actually enforced?	Configure your directory or identity platform to enforce the defined waiting period. Document deprovisioned accounts with their disable date so the waiting period can be tracked and verified during an assessment.
IA.L2-3.5.6	**[a]**	A period of inactivity after which an identifier is disabled is defined	Have you defined how long an account can be inactive before it gets disabled?	Define in your account management policy how many days of inactivity trigger account disablement. Ninety days is a common threshold - align it with your organizational risk tolerance and document the rationale.
IA.L2-3.5.6	**[b]**	Identifiers are disabled after the defined period of inactivity	Are accounts that have not been used in that period actually being disabled?	Configure your identity platform or run periodic account review scripts to automatically disable accounts that meet the inactivity threshold. HR system integration helps catch terminations that IT might otherwise miss.
IA.L2-3.5.7	**[a]**	Password complexity requirements are defined	Have you set rules for what makes a password strong enough - length, character types, etc.?	Document minimum password complexity requirements in your security policy - minimum length, required character types, or a passphrase approach. Be specific enough that configurations can be validated against the policy.
IA.L2-3.5.7	**[b]**	Password change of character requirements are defined	Have you defined how different a new password must be from the previous one when changed?	Define how much a new password must differ from the previous one when changed - for example, at least four different characters. Document this alongside your complexity requirements.
IA.L2-3.5.7	**[c]**	Minimum password complexity requirements as defined are enforced when new passwords are created	When users create passwords, does the system actually enforce those complexity rules?	Configure your identity provider to enforce complexity rules when new passwords are created. Test by attempting to set a non-compliant password to confirm the rule is actually being enforced.
IA.L2-3.5.7	**[d]**	Minimum password change of character requirements as defined are enforced when new passwords are created	When users change passwords, does the system verify the new one is different enough from the old one?	Configure your identity provider to check that new passwords differ sufficiently from the previous one. This is typically a setting alongside the password history configuration in your directory.
IA.L2-3.5.8	**[a]**	The number of generations during which a password cannot be reused is specified	Have you defined how many previous passwords the system remembers so users cannot just recycle old ones?	Define how many previous passwords the system must remember. NIST and common practice suggest at least the last 24. Document this number in your password policy so it can be validated against your system settings.
IA.L2-3.5.8	**[b]**	Reuse of passwords is prohibited during the specified number of generations	Does the system actually prevent users from reusing recent passwords?	Configure password history in your Active Directory, identity provider, or application authentication settings. Test to confirm users cannot successfully reuse a recent password by attempting a reuse during testing.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IA.L2-3.5.9	[a]	An immediate change to a permanent password is required when a temporary password is used for system logon	When someone receives a temporary password, are they required to change it the first time they log in?	Configure the force-change-at-next-login flag in your identity platform for all temporary and reset passwords. Build this into your help desk procedures so it happens consistently every time a reset is issued.
IA.L2-3.5.10	[a]	Passwords are cryptographically protected in storage	Are passwords stored in your systems protected by strong cryptographic hashing - not sitting in plain text?	Ensure your systems use salted cryptographic hashing for stored passwords. Audit any custom-built or legacy applications - these are most likely to have insecure storage implementations. Plain-text or reversible storage is a critical finding.
IA.L2-3.5.10	[b]	Passwords are cryptographically protected in transit	Are passwords encrypted when they travel across a network?	Verify that all password authentication occurs over encrypted connections - TLS for web applications, LDAPS for directory lookups. Block any unencrypted protocols that could expose credentials in transit.
IA.L2-3.5.11	[a]	Authentication information is obscured during the authentication process	When someone types a password or code, is it masked on screen so it cannot be read by someone nearby?	Verify that all login interfaces mask password and authentication input. Modern systems do this by default, but legacy or custom-built applications may still display input in clear text. Test each login interface to confirm masking is working.

Incident Response (IR)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IR.L2-3.6.1	[a]	An operational incident-handling capability is established	Do you have a working, active incident response capability - not just a plan sitting on a shelf?	Create an incident response plan and operationalize it - assign roles, acquire tools, run a test exercise. An IR retainer with a third-party security firm can supplement internal capability if your team is small.
IR.L2-3.6.1	[b]	The operational incident-handling capability includes preparation	Are the right people trained and the right tools ready before an incident ever happens?	Preparation means trained people, documented playbooks, and the right tools ready before an incident. Run tabletop exercises, maintain contact lists, and keep playbooks current with your actual environment.
IR.L2-3.6.1	[c]	The operational incident-handling capability includes detection	Do you have a way to actually detect incidents - not just wait for someone to report a problem?	Deploy detection capabilities - EDR, SIEM, and IDS/IPS at minimum. Alerts need to route to someone who can actually respond, not just accumulate in a system nobody is actively monitoring.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IR.L2-3.6.1	**[d]**	The operational incident-handling capability includes analysis	Can you analyze a security incident to figure out what happened, how bad it is, and why?	Define your analysis process - how do you triage an alert, determine if it is a real incident, assess scope, and identify affected systems? Playbooks for common scenarios significantly speed this up.
IR.L2-3.6.1	**[e]**	The operational incident-handling capability includes containment	Can you contain an active incident to stop it from spreading further?	Containment playbooks should define how to isolate affected systems, revoke compromised credentials, and block malicious activity. Tailor them to the most likely scenarios for your specific environment.
IR.L2-3.6.1	**[f]**	The operational incident-handling capability includes recovery	Can you recover your systems and get back to normal after an incident?	Recovery procedures should cover restoring from backup, validating system integrity, and returning to normal operations. Test your recovery capability before you need it - not during an actual incident.
IR.L2-3.6.1	**[g]**	The operational incident-handling capability includes user response activities	Do employees know what to report and who to contact when something looks wrong?	Train end users on what to report and who to contact when something looks wrong. A simple, memorable reporting path - a dedicated email address or phone number - increases the likelihood employees actually report suspicious activity.
IR.L2-3.6.2	**[a]**	Incidents are tracked	Are security incidents being tracked and logged - not just handled and forgotten?	Use an incident tracking system - ticketing platform, spreadsheet, or dedicated IR tool - to log every security incident. Each event gets a record regardless of how minor it seems at the time.
IR.L2-3.6.2	**[b]**	Incidents are documented	Is each incident documented with enough detail to support a review or investigation?	Each incident record should include at minimum: what happened, when it was detected, which systems were affected, who responded, and what actions were taken. Enough detail to support a post-incident review.
IR.L2-3.6.2	**[c]**	Authorities to whom incidents are to be reported are identified	Have you identified which external authorities need to be notified of incidents - like CISA or your prime contractor?	Identify in your IR plan which external authorities must be notified - CISA, your prime contractor, the Contracting Officer. Know the notification timelines required for each - some contracts require notification within 72 hours.
IR.L2-3.6.2	**[d]**	Organizational officials to whom incidents are to be reported are identified	Have you identified which internal leaders and stakeholders need to be informed when an incident occurs?	Identify which internal stakeholders must be informed - legal, executive leadership, HR, IT management. Put the notification chain in writing so there is no ambiguity during a real incident.
IR.L2-3.6.2	**[e]**	Identified authorities are notified of incidents	Are the required external authorities actually being notified when incidents happen?	When an incident occurs, follow the defined notification procedure and document that notifications were sent, to whom, and when. Timeliness is part of what gets evaluated - late notifications are a finding.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
IR.L2-3.6.2	[f]	Identified organizational officials are notified of incidents	Are the required internal people actually being notified?	Notify the defined internal stakeholders as part of your incident response workflow. Log all notifications in your incident record alongside the timeline of events.
IR.L2-3.6.3	[a]	The incident response capability is tested	Do you periodically test your incident response plan - through exercises or simulations - to see if it would actually work?	Run an annual tabletop exercise using a realistic scenario - ransomware, phishing-based breach, or insider threat. Document results, identify gaps, update playbooks, and keep the after-action report as evidence.

Maintenance (MA)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
MA.L2-3.7.1	[a]	System maintenance is performed	Is system maintenance actually being performed and documented, with records to prove it?	Keep maintenance records - patching logs, vendor service reports, ITSM tickets. The assessor wants to see evidence that maintenance is actively happening, not just that a policy exists saying it should be done.
MA.L2-3.7.2	[a]	Tools used to conduct system maintenance are controlled	Are the tools used for maintenance approved and controlled - not just whatever someone brings in?	Maintain an approved tools list and require any maintenance tool to be on it before use. Unvetted software brought in by vendors or contractors is a common malware infection vector that this control is specifically designed to address.
MA.L2-3.7.2	[b]	Techniques used to conduct system maintenance are controlled	Are the techniques used during maintenance approved and controlled?	Document approved maintenance techniques - remote access methods, diagnostic approaches, testing procedures - so maintenance activities are consistent and controlled regardless of who is performing them.
MA.L2-3.7.2	[c]	Mechanisms used to conduct system maintenance are controlled	Are the mechanisms used during maintenance approved and controlled?	Define and document the approved mechanisms - specific software versions, hardware tools, diagnostic platforms - used during maintenance activities. This goes alongside the approved tools list.
MA.L2-3.7.2	[d]	Personnel used to conduct system maintenance are controlled	Are the people doing maintenance - especially outside vendors - vetted and supervised?	Vet maintenance personnel before granting access. For outside vendors, review their security posture and require an NDA. Supervise anyone who does not have pre-authorized access to your systems.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
MA.L2-3.7.3	[a]	Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI	Before equipment leaves your building for off-site repair, is any sensitive data on it wiped first?	Before any device leaves the building for service, follow NIST 800-88 sanitization procedures - full disk overwrite, cryptographic erase, or physical destruction. Obtain and retain a sanitization certificate as evidence.
MA.L2-3.7.4	[a]	Media containing diagnostic and test programs are checked for malicious code before being used in organizational systems	Are diagnostic disks or USB drives brought in for maintenance scanned for malware before being used on your systems?	Before any diagnostic USB, disk, or tool is plugged into your systems, run a malware scan using an approved endpoint protection tool. Maintain a controlled set of pre-approved maintenance media where possible.
MA.L2-3.7.5	[a]	Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections	When someone performs maintenance remotely, do they have to use MFA to establish that connection?	Require MFA to establish any remote maintenance session - through VPN, ZTNA, or a remote access tool. Treat remote maintenance access as a privileged session requiring the same authentication standards.
MA.L2-3.7.5	[b]	Nonlocal maintenance sessions are terminated when nonlocal maintenance is complete	When remote maintenance is done, is the session closed - not left open indefinitely?	Define when a remote maintenance session must be terminated - when work is complete or after a maximum duration. Configure automatic session termination so it does not rely on the technician manually disconnecting.
MA.L2-3.7.6	[a]	Maintenance personnel without required access authorization are supervised during maintenance activities	If a maintenance person does not have full access authorization, are they supervised at all times while working?	If a maintenance person does not have pre-authorized access, assign an escort before they begin. Monitor what they access and what actions they take. Use temporary accounts with a defined expiration date.

Media Protection (MP)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
MP.L2-3.8.1	[a]	Paper media containing CUI is physically controlled	Are paper documents containing sensitive data physically secured?	Require paper documents containing CUI to be stored in locked cabinets or secure areas when not in use. Define who has key or combination access and keep that list current with your personnel changes.
MP.L2-3.8.1	[b]	Digital media containing CUI is physically controlled	Are drives and digital media containing sensitive data physically secured?	Treat digital media the same as paper - drives, USB sticks, and other media containing CUI should be in locked, access-controlled locations when not actively being used.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
MP.L2-3.8.1	**[c]**	Paper media containing CUI is securely stored	Are sensitive paper documents stored safely when not in use?	Establish locked storage for CUI paper documents - locked file cabinets, safes, or secure rooms. Pair this with a clean desk policy so paper is not left unattended on desks overnight or during absences.
MP.L2-3.8.1	**[d]**	Digital media containing CUI is securely stored	Is digital media with sensitive data stored safely - not left on desks or in unlocked locations?	Establish locked storage for digital media - a locked cabinet, safe, or controlled server room. Do not leave media containing CUI in unlocked desk drawers, common areas, or on top of desks.
MP.L2-3.8.2	**[a]**	Access to CUI on system media is limited to authorized users	Is access to drives and media containing sensitive data restricted to only authorized people?	Document who is authorized to handle CUI media. Enforce access through physical controls - locked storage with limited keyholders - and encryption on digital media so even physical access does not expose the data.
MP.L2-3.8.3	**[a]**	System media containing CUI is sanitized or destroyed before disposal	When disposing of drives or devices, is sensitive data permanently destroyed before they leave your control?	Follow NIST 800-88 for sanitization and destruction. Use certified destruction services for physical media and obtain certificates of destruction. Maintain records of every device that is disposed of.
MP.L2-3.8.3	**[b]**	System media containing CUI is sanitized before it is released for reuse	Before a drive is reused by someone new, is all sensitive data wiped from it first?	Before reassigning a drive or device to a new user, perform a full wipe using NIST 800-88 methods. Standard deletion or quick format is not sufficient - data can be recovered from improperly sanitized media.
MP.L2-3.8.4	**[a]**	Media containing CUI is marked with applicable CUI markings	Is media containing sensitive data labeled so people know what is on it and how to handle it?	Label all CUI media with the appropriate CUI marking - the document category, handling instructions, and any special markings required for that CUI category. Use consistent templates so labeling is uniform.
MP.L2-3.8.4	**[b]**	Media containing CUI is marked with distribution limitations	Does the label also indicate who is allowed to receive it or any restrictions on distribution?	Include distribution limitation statements on all CUI labels - such as contractor-only handling or specific authorized recipient lists. The label should tell anyone who picks it up exactly how to handle it.
MP.L2-3.8.5	**[a]**	Access to media containing CUI is controlled	Is access to drives or media containing sensitive data actively controlled?	Control who can access, check out, or move CUI media through an access log or checkout process. Assign a custodian responsible for tracking CUI media so there is always a clear owner.
MP.L2-3.8.5	**[b]**	Accountability for media containing CUI is maintained during transport outside of controlled areas	When sensitive media is transported, is there a chain of custody tracking where it went and who had it?	When CUI media travels outside your facility, maintain a chain-of-custody log documenting every handoff. Use tracking numbers, tamper-evident packaging, and require acknowledgment of receipt at the destination.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
MP.L2-3.8.6	**[a]**	The confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards	When portable drives with sensitive data need to be transported, are they encrypted or physically protected?	Use FIPS-validated encrypted drives for transporting CUI on portable media. If physical safeguards are used instead, document exactly what they are and why they meet the requirement. Encryption is simpler and more defensible.
MP.L2-3.8.7	**[a]**	The use of removable media on system components is controlled	Are there controls over which removable devices can be plugged into your systems - not just any USB someone brings in?	Use endpoint device control tools to define which USB devices are allowed on your systems - by device class, manufacturer, or specific device ID. Block anything not on the approved list automatically at the endpoint.
MP.L2-3.8.8	**[a]**	The use of portable storage devices is prohibited when such devices have no identifiable owner	Are employees prohibited from using portable storage devices with no identifiable owner?	Combine a clear policy prohibiting ownerless devices with technical USB blocking that prevents any device without a tracked, identified owner from connecting. Training reinforces why this matters.
MP.L2-3.8.9	**[a]**	The confidentiality of backup CUI is protected at storage locations	Are backup copies of sensitive data encrypted or otherwise protected where they are stored?	Encrypt backups using FIPS-validated cryptography and restrict access to backup storage. Immutable backup configurations protect against ransomware tampering. Test restoration procedures regularly to confirm backups are actually usable.

Personnel Security (PS)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
PS.L2-3.9.1	**[a]**	Individuals are screened prior to authorizing access to organizational systems containing CUI	Are employees screened - such as through a background check - before being given access to systems that handle sensitive data?	Define background check requirements in your HR policy before granting access to systems handling CUI. Document screening completion as part of onboarding records. The level of screening should reflect the sensitivity of the access.
PS.L2-3.9.2	**[a]**	A policy and/or process for terminating system access and any credentials coincident with personnel actions is established	Do you have a documented process to revoke access and credentials when someone leaves or changes roles?	Document a formal offboarding process that includes account deprovisioning, badge revocation, credential rotation, and equipment return. An HR-to-IT integration or automated workflow ensures nothing is missed when someone leaves.
PS.L2-3.9.2	**[b]**	System access and credentials are terminated consistent with personnel actions such as termination or transfer	Is access actually removed promptly when someone is terminated or transferred?	Execute the offboarding process promptly when someone is terminated or transfers. Configure automated deprovisioning triggers tied to HR status changes where possible - delays in removing access are a common and significant gap.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
PS.L2-3.9.2	[c]	The system is protected during and after personnel transfer actions	Are systems protected during and after those personnel transitions - no lingering access gaps?	After a departure, conduct a brief review to confirm all access was removed and no residual credentials or sessions remain active. This step is easy to skip under time pressure but important to prevent lingering unauthorized access.

Physical Protection (PE)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
PE.L2-3.10.1	[a]	Authorized individuals allowed physical access are identified	Have you identified who is allowed to physically access areas where your systems or sensitive data are located?	Maintain a documented access list for secure areas and tie it to your badge access system so it is enforced automatically. Review and update it regularly - especially after personnel changes.
PE.L2-3.10.1	[b]	Physical access to organizational systems is limited to authorized individuals	Is physical access to your systems limited to those approved individuals?	Configure badge access controls to allow only approved individuals into spaces where systems are located. Review and update the access list at least quarterly to catch stale access.
PE.L2-3.10.1	[c]	Physical access to equipment is limited to authorized individuals	Is physical access to equipment also limited to authorized people?	Apply the same access controls to equipment - not just room entry, but server racks, storage systems, and networking gear. Lock cabinets and equipment cages where appropriate.
PE.L2-3.10.1	[d]	Physical access to operating environments is limited to authorized individuals	Is physical access to server rooms and secure operating areas restricted to authorized personnel?	Define and protect your operating environments - any space where CUI is processed or stored. This includes office areas where CUI is regularly worked on, not just dedicated server rooms.
PE.L2-3.10.2	[a]	The physical facility where organizational systems reside is protected	Is your physical facility protected from unauthorized entry?	Physical access controls, locks, and badge systems protect the facility. Supplement with a security culture - tailgating awareness training and a clearly communicated visitor policy that all employees understand.
PE.L2-3.10.2	[b]	The support infrastructure for organizational systems is protected	Is the supporting infrastructure - power, cooling, and cabling - also physically protected?	Protect power distribution units, cooling systems, and network cabling from unauthorized access. Disrupting supporting infrastructure can take down your environment as effectively as attacking the systems themselves.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
PE.L2-3.10.2	**[c]**	The physical facility where organizational systems reside is monitored	Is your facility actively monitored through cameras, alarms, or security patrols?	Deploy cameras and motion detection in and around secure areas. Review footage on a defined schedule and retain recordings for a defined retention period. Integrate with your physical access system for correlated alerts.
PE.L2-3.10.2	**[d]**	The support infrastructure for organizational systems is monitored	Is supporting infrastructure also monitored for disruption or tampering?	Monitor supporting infrastructure through environmental sensors - temperature, humidity, water detection, and power quality. Many server room and data center management platforms include these capabilities as standard features.
PE.L2-3.10.3	**[a]**	Visitors are escorted	Are visitors escorted at all times in areas where systems or sensitive data are present?	Require all visitors to sign in, receive a visible visitor badge, and be assigned an escort before entering any area where systems or CUI are present. Apply this consistently - even for familiar vendors or contractors.
PE.L2-3.10.3	**[b]**	Visitor activity is monitored	Is visitor activity actively monitored while they are on site?	Assign escorts who actively monitor visitor activity throughout the visit, not just walk them to a room and leave. Camera coverage supplements escort monitoring and provides an independent record of what occurred.
PE.L2-3.10.4	**[a]**	Audit logs of physical access are maintained	Are records kept of who physically accessed your facilities and systems?	Badge access systems automatically generate physical access logs. For areas without electronic control, maintain a paper sign-in log. Retain records for your defined retention period and confirm they are accessible during an assessment.
PE.L2-3.10.5	**[a]**	Physical access devices are identified	Have you inventoried all physical access devices - badges, keys, and access cards?	Maintain an inventory of every physical access device - badges, keys, access cards, lock combinations. Include who was issued each item, when it was issued, and the associated access level.
PE.L2-3.10.5	**[b]**	Physical access devices are controlled	Are those devices actively managed - no untracked keys or active badges for people who have left?	Actively manage that inventory - immediately deactivate badges and change combinations when someone with access leaves or changes roles. Do not wait for the next scheduled review to address departures.
PE.L2-3.10.5	**[c]**	Physical access devices are managed	Are physical access devices managed through their full lifecycle - issued, tracked, and revoked when no longer needed?	Conduct periodic reviews of your physical access device inventory - at least annually. Verify that active badges and keys match your current approved access list and that no orphaned access remains for people who have left.
PE.L2-3.10.6	**[a]**	Safeguarding measures for CUI are defined for alternate work sites	Have you defined rules for how sensitive data must be protected when employees work from home or a remote location?	Define specific rules for remote work in a written policy - required VPN use, encrypted device requirements, clean desk expectations, prohibition on printing CUI at home, and secure storage of any physical materials.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
PE.L2-3.10.6	**[b]**	Safeguarding measures for CUI are enforced for alternate work sites	Are those remote work protection rules actually being followed?	Enforce the requirements technically where possible - VPN settings, MDM compliance checks, full-disk encryption requirements. For requirements that cannot be technically enforced, rely on training, acknowledgement, and periodic spot checks.

Risk Assessment (RA)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
RA.L2-3.11.1	**[a]**	The frequency to assess risk to organizational operations, organizational assets, and individuals is defined	Have you defined how often you will formally assess the risks to your systems and operations?	Define a risk assessment schedule in your security policy and SSP - annually is the baseline. Document it formally so the commitment is visible to assessors and drives actual execution.
RA.L2-3.11.1	**[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	Are those risk assessments actually being conducted on schedule?	Conduct the risk assessment on schedule using a defined methodology - likelihood and impact ratings for each identified risk. Document findings in a risk register and get leadership sign-off. The output feeds your POA&M.
RA.L2-3.11.2	**[a]**	The frequency to scan for vulnerabilities in organizational systems and applications is defined	Have you defined how often vulnerability scans need to run on your systems and applications?	The organization must define an appropriate scanning frequency based on its environment and risk. Monthly or quarterly scanning may be reasonable in some environments, but CMMC does not prescribe a specific interval. Document the tools you use alongside the defined schedule.
RA.L2-3.11.2	**[b]**	Vulnerability scans are performed on organizational systems with the defined frequency	Are vulnerability scans actually running on your systems at that frequency?	Configure scheduled authenticated scans for your systems using a vulnerability scanner. Authenticated scans produce significantly more accurate results than unauthenticated ones. Retain scan reports as assessment evidence.
RA.L2-3.11.2	**[c]**	Vulnerability scans are performed on applications with the defined frequency	Are vulnerability scans also running on your applications at that frequency?	Include application scanning in your program - web application scanners or DAST tools on a defined schedule. Application vulnerabilities are often missed when organizations focus only on infrastructure scanning.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
RA.L2-3.11.2	**[d]**	Vulnerability scans are performed on organizational systems when new vulnerabilities are identified	When a new vulnerability is publicly disclosed, do you scan your systems to see if you are affected?	Subscribe to vulnerability disclosure feeds - CISA KEV, vendor security bulletins, NVD. When a new critical CVE is published, trigger an immediate scan to determine if your systems are exposed before attackers find them.
RA.L2-3.11.2	**[e]**	Vulnerability scans are performed on applications when new vulnerabilities are identified	When a new vulnerability is disclosed, do you also scan your applications?	Apply the same event-triggered scan requirement to your applications when new vulnerabilities relevant to your technology stack are disclosed publicly.
RA.L2-3.11.3	**[a]**	Vulnerabilities are identified	Are identified vulnerabilities being catalogued and tracked?	Route scan results into a vulnerability management platform or ticketing system where every finding is catalogued with severity, affected system, and discovery date. Nothing should fall through the cracks.
RA.L2-3.11.3	**[b]**	Vulnerabilities are remediated in accordance with risk assessments	Are vulnerabilities being fixed in order of risk - the most dangerous ones first?	Prioritize remediation by risk - CVSS score and exploitability - not just by age or convenience. Define SLAs for remediation timelines by severity and track compliance. Document formal risk acceptance when immediate remediation is not possible.

Security Assessment (CA)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CA.L2-3.12.1	**[a]**	The frequency of security control assessments is defined	Have you defined how often your security controls need to be formally tested?	Define your assessment frequency in your security policy and SSP - annually is the minimum. Specify whether assessments will be internal, third-party, or a combination, and document the rationale.
CA.L2-3.12.1	**[b]**	Security controls are assessed with the defined frequency to determine if the controls are effective in their application	Are those assessments actually happening on schedule to confirm controls are working?	Execute assessments on schedule, collecting actual evidence that controls are working - configuration screenshots, log samples, test results. An assessor reviewing real evidence is very different from reading a policy document.
CA.L2-3.12.2	**[a]**	Deficiencies and vulnerabilities to be addressed by the plan of action are identified	Have you identified and documented the gaps and weaknesses in your security program?	Maintain a POA&M that captures every known gap - from assessments, vulnerability scans, or self-identified weaknesses. Each item needs a description, risk level, responsible owner, and target date. Keep it current and honest.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CA.L2-3.12.2	**[b]**	A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities	Is there a formal plan with owners and deadlines to address those gaps?	Develop remediation plans for each POA&M item with realistic milestones and assigned owners. The plan is your commitment to fix - assessors will review it for completeness and credibility, so vague entries undermine your posture.
CA.L2-3.12.2	**[c]**	The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities	Is that remediation plan actively being worked - not just documented and left on a shelf?	Actually work the POA&M - update status regularly, track progress against milestones, and close items when remediated. POA&M items with no movement in months are a red flag that will draw assessor attention.
CA.L2-3.12.3	**[a]**	Security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls	Are your security controls monitored on an ongoing basis between formal assessments?	Do not wait for annual assessments to know whether controls are working. Use continuous monitoring tools - vulnerability scanners, SIEM dashboards, configuration compliance checks - to track control health on an ongoing basis.
CA.L2-3.12.4	**[a]**	A system security plan is developed	Do you have a written System Security Plan describing how you meet each security requirement?	Write or commission an SSP that covers all 110 CMMC Level 2 requirements. This is your foundational compliance document – it needs to be complete, accurate, and actually reflect how your environment works in practice.
CA.L2-3.12.4	**[b]**	The system boundary is described and documented in the system security plan	Does the SSP clearly define your system boundary - what is in scope and what is not?	Define your system boundary clearly in network diagrams and the SSP - what is in scope, what is excluded, and why. A well-defined boundary makes the rest of the assessment more manageable and defensible.
CA.L2-3.12.4	**[c]**	The system environment of operation is described and documented in the system security plan	Does the SSP describe the environment your systems operate in?	Describe your operating environment in detail in the SSP - cloud platforms, on-prem infrastructure, managed services, and remote access methods. The assessor needs to understand your environment to evaluate your controls.
CA.L2-3.12.4	**[d]**	The security requirements identified and approved by the designated authority as non-applicable are identified	Are requirements that do not apply to your environment formally identified and approved in the SSP?	For any CMMC requirement that does not apply to your environment, document the rationale and get approval from your designated authority. Blanket non-applicability claims without documentation will not hold up to scrutiny.
CA.L2-3.12.4	**[e]**	The method of security requirement implementation is described and documented in the system security plan	Does the SSP explain how you are meeting each specific security requirement?	For each requirement, describe specifically how you meet it in the SSP - not just that you have a firewall, but which firewall, how it is configured, and what it protects. Vague descriptions create doubt.
CA.L2-3.12.4	**[f]**	The relationship with or connection to other systems is described and documented in the system security plan	Does the SSP document how your systems connect to or interact with other systems?	Document system interconnections in the SSP - what external systems connect to your environment, how connections are secured, and what data flows across them. System interconnection agreements formalize these relationships.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
CA.L2-3.12.4	[g]	The frequency to update the system security plan is defined	Have you defined how often the SSP gets reviewed and updated?	Define how often your SSP is reviewed and updated in the plan itself - at least annually or when significant changes occur. Make this a standing agenda item in your security program calendar.
CA.L2-3.12.4	[h]	System security plan is updated with the defined frequency	Is the SSP actually being updated on that defined schedule?	Actually update the SSP on that schedule. A stale SSP that no longer reflects your environment is worse than no SSP – it creates contradictions an assessor will notice and question immediately.

System and Communications Protection (SC)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SC.L2-3.13.1	[a]	The external system boundary is defined	Have you defined where your external system boundary is - the perimeter between your environment and the outside world?	Define your external system boundary in your network documentation and SSP - the perimeter between your environment and the outside world, including internet connections, cloud entry points, and partner connections.
SC.L2-3.13.1	[b]	Key internal system boundaries are defined	Have you also defined key internal boundaries - like the line between your sensitive networks and general office networks?	Define key internal boundaries too - particularly the line between networks handling CUI and those that do not. Network segmentation is the technical implementation that makes these boundaries real, not just diagrammed.
SC.L2-3.13.1	[c]	Communications are monitored at the external system boundary	Is traffic crossing your external boundary being monitored so you can see what is coming in and going out?	Deploy monitoring at your external boundary – firewall logs, IDS/IPS, flow data. Route these into your SIEM for visibility into what is entering and exiting your environment on an ongoing basis.
SC.L2-3.13.1	[d]	Communications are monitored at key internal boundaries	Is traffic crossing internal boundaries also being monitored for suspicious activity?	Monitor internal boundary traffic too. Lateral movement - attackers moving between internal segments - is often more damaging than initial intrusion and much harder to detect without internal monitoring in place.
SC.L2-3.13.1	[e]	Communications are controlled at the external system boundary	Is traffic at your external boundary actively controlled - not just observed?	Enforce traffic controls at your external boundary through firewall rules and access control lists. Review rules regularly to remove stale or overly permissive entries that have accumulated over time.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SC.L2-3.13.1	[f]	Communications are controlled at key internal boundaries	Is traffic at internal boundaries also controlled, not just monitored?	Enforce controls at internal boundaries through internal firewalls, VLANs, and microsegmentation. Limit east-west traffic between segments to only what is specifically necessary for business operations.
SC.L2-3.13.1	[g]	Communications are protected at the external system boundary	Are communications at your external boundary protected from unauthorized access or tampering?	Protect external boundary communications through encryption and integrity controls. Ensure traffic is authenticated before being admitted into your environment - unauthenticated inbound connections are an unnecessary risk.
SC.L2-3.13.1	[h]	Communications are protected at key internal boundaries	Are communications at internal boundaries also protected?	Apply the same protections to internal boundary communications. Encrypting internal traffic is especially important for any segment that handles or transmits CUI.
SC.L2-3.13.2	[a]	Architectural designs that promote effective information security are identified	Have you identified security-focused design principles used when building your systems?	Document which security architecture principles you apply - defense in depth, zero trust, least privilege by design. Your architecture should visibly reflect these principles, not just your policy documents.
SC.L2-3.13.2	[b]	Software development techniques that promote effective information security are identified	Have you identified secure software development practices your team follows?	If you develop software, document secure coding standards - OWASP Top 10, input validation, error handling, code review. If you procure software, require vendors to demonstrate they follow secure development practices.
SC.L2-3.13.2	[c]	Systems engineering principles that promote effective information security are identified	Have you identified secure systems engineering principles applied during design and build?	Document the systems engineering principles you apply when designing systems - fail-safe defaults, complete mediation, separation of privilege. These should be reflected in your architecture and design reviews.
SC.L2-3.13.2	[d]	Identified architectural designs that promote effective information security are employed	Are those secure architectural designs actually being used - not just identified on paper?	Show that secure architecture principles are actually reflected in your systems - network diagrams, architecture documents, and configuration evidence demonstrate this is more than a policy commitment.
SC.L2-3.13.2	[e]	Identified software development techniques that promote effective information security are employed	Are those secure development practices actually being followed?	Show that secure coding practices are being followed through code review records, static analysis scan results, or penetration testing findings. Evidence of practice matters more than evidence of policy.
SC.L2-3.13.2	[f]	Identified systems engineering principles that promote effective information security are employed	Are those engineering principles actually being applied in practice?	Show that systems engineering principles are applied in practice through design review documentation, change management records, and technical configuration evidence.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SC.L2-3.13.3	**[a]**	User functionality is identified	Have you defined what regular users do in your systems?	Define user-facing functions - the applications and capabilities regular employees use day to day. These are what standard user accounts should be able to reach.
SC.L2-3.13.3	**[b]**	System management functionality is identified	Have you defined what system administration functions look like and who performs them?	Define system management functions - admin consoles, configuration interfaces, monitoring tools, and privileged utilities. These should only be reachable by designated admin accounts using dedicated connections.
SC.L2-3.13.3	**[c]**	User functionality is separated from system management functionality	Are user functions and admin functions separated so the same person cannot do both from the same account?	Separate user and admin functions technically through separate accounts, networks, or admin jump servers. The same account and connection should not be used for both everyday work and system administration.
SC.L2-3.13.4	**[a]**	Unauthorized and unintended information transfer via shared system resources is prevented	Are shared system resources controlled so one user cannot read data left behind by another through memory or shared storage?	Keep OS and virtualization platforms patched - many shared resource vulnerabilities are addressed through patching alone. Configure OS-level memory isolation and apply hypervisor security settings to prevent cross-tenant data exposure.
SC.L2-3.13.5	**[a]**	Publicly accessible system components are identified	Have you identified which of your systems are publicly accessible - like web portals or APIs?	Identify all system components accessible from the internet or untrusted networks - web servers, email gateways, public portals, APIs. Document them in your network inventory with their exposure level noted.
SC.L2-3.13.5	**[b]**	Subnetworks for publicly accessible system components are physically or logically separated from internal networks	Are those public-facing components isolated from your internal systems on a separate network segment?	Place those public-facing components in a DMZ or separate network segment isolated from your internal CUI environment. Firewall rules should prevent direct communication between the DMZ and systems containing CUI.
SC.L2-3.13.6	**[a]**	Network communications traffic is denied by default	Is all network traffic blocked by default unless it has been explicitly approved?	Configure your firewalls and network controls with a default-deny stance - no traffic is permitted unless explicitly allowed. This requires reviewing and justifying every existing firewall rule, which is often overdue.
SC.L2-3.13.6	**[b]**	Network communications traffic is allowed by exception	Is traffic only permitted when specifically authorized - nothing gets through unless allowed?	Document each permitted traffic flow and its business justification. Treat firewall rule reviews as periodic maintenance - remove rules that no longer serve a business purpose rather than letting them accumulate.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SC.L2-3.13.7	**[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	When employees connect via VPN, are they prevented from simultaneously browsing the internet directly?	Disable split tunneling in your VPN client configuration so all traffic - including internet-bound traffic - routes through your corporate gateway when an employee is connected. This ensures your security controls apply universally.
SC.L2-3.13.8	**[a]**	Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified	Have you identified which encryption tools or protocols protect sensitive data while it is being sent?	Document which encryption tools and protocols protect CUI in transit - TLS version and cipher suites for web traffic, SFTP for file transfers, encrypted email for messaging. Virtru directly addresses email and file sharing by encrypting CUI so only authorized recipients can open it, even after delivery.
SC.L2-3.13.8	**[b]**	Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified	Have you identified any physical safeguards being used in place of or alongside encryption for data in transit?	If physical safeguards are used instead of or alongside encryption for certain transmission scenarios, document what those safeguards are and why they are considered an equivalent level of protection.
SC.L2-3.13.8	**[c]**	Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission	Is encryption or an approved physical alternative actually protecting sensitive data during transmission?	Verify that encryption or approved physical safeguards are actually in place and functioning - not just planned or documented. Configuration screenshots, TLS scan results, and Virtru audit logs showing encrypted delivery are all valid forms of evidence.
SC.L2-3.13.9	**[a]**	A period of inactivity to terminate network connections associated with communications sessions is defined	Have you defined how long a network connection can sit idle before it is automatically ended?	Define an inactivity timeout period for network connections in your policy - 15 to 30 minutes for user sessions is a common range. Document this so it can be validated against actual system configurations.
SC.L2-3.13.9	**[b]**	Network connections associated with communications sessions are terminated at the end of the sessions	Are network connections closed when a session is complete - not left open indefinitely?	Configure your applications, VPN, and network devices to close connections when a session ends normally - not just on timeout. Sessions that stay open after the user finishes work are an unnecessary exposure.
SC.L2-3.13.9	**[c]**	Network connections associated with communications sessions are terminated after the defined period of inactivity	Are idle connections actually being terminated after the defined inactivity period?	Configure idle session timeout in your VPN, application servers, and network infrastructure. Test to confirm connections are actually terminated after the defined inactivity period - not just that the setting appears correct.
SC.L2-3.13.10	**[a]**	Cryptographic keys are established whenever cryptography is employed	When you use encryption, is there a proper process for generating cryptographic keys - not just relying on defaults?	Use a Key Management System or HSM to generate cryptographic keys using approved random generation methods. Avoid generating keys manually or relying on default keys provided by vendors out of the box.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SC.L2-3.13.10	[b]	Cryptographic keys are managed whenever cryptography is employed	Are those keys managed throughout their lifecycle - rotated, stored securely, and revoked when no longer needed?	Define and follow a key management lifecycle - rotation schedules, secure storage, backup copies, revocation procedures. Document this in a key management plan. Weak key management undermines even strong encryption algorithms.
SC.L2-3.13.11	[a]	FIPS-validated cryptography is employed to protect the confidentiality of CUI	When encryption is used to protect sensitive data, is it using FIPS 140-2 or 140-3 validated modules - not just any encryption tool?	Verify that all encryption protecting CUI confidentiality uses FIPS 140-2 or 140-3 validated modules. Check the NIST CMVP database to confirm your specific product and version are listed. Virtru uses FIPS-validated cryptography and directly supports email and file sharing scenarios where this requirement applies.
SC.L2-3.13.12	[a]	Collaborative computing devices are identified	Have you identified all cameras, microphones, and smart boards in areas where sensitive data is discussed?	Maintain an inventory of all cameras, microphones, smart speakers, and collaborative displays in areas where CUI is discussed. This includes conference room equipment and personal devices brought into those spaces.
SC.L2-3.13.12	[b]	Collaborative computing devices provide indication to users of devices in use	Do those devices have a visible or audible indicator showing when they are actively in use?	Verify that all collaborative devices have a visible or audible indicator showing when they are actively in use. Test each device to confirm the indicator works and is visible to people in the room.
SC.L2-3.13.12	[c]	Remote activation of collaborative computing devices is prohibited	Is it possible for someone to turn those devices on remotely without the user knowing?	Review device settings and management policies to confirm remote activation features are disabled. If remote administration is required for legitimate purposes, require explicit local consent before any remote activation occurs.
SC.L2-3.13.13	[a]	Use of mobile code is controlled	Is mobile code - like browser scripts or downloadable applets - running on your systems approved and controlled?	Define a policy for mobile code - which types are permitted, which are prohibited, and how exceptions are handled. Browser security settings, endpoint protection, and application control tools enforce the policy technically.
SC.L2-3.13.13	[b]	Use of mobile code is monitored	Is mobile code activity being monitored so you know what is executing on your systems?	Route mobile code activity through monitoring tools - EDR, web proxies, or endpoint security platforms - so you have ongoing visibility into what is actually executing on your systems.
SC.L2-3.13.14	[a]	Use of Voice over Internet Protocol (VoIP) technologies is controlled	Is use of VoIP systems in your environment approved and controlled?	Approve and document which VoIP systems are permitted in your environment. Configure them securely - encrypted voice traffic, strong authentication for admin access, and regular patching as part of your standard maintenance cycle.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SC.L2-3.13.14	**[b]**	Use of Voice over Internet Protocol (VoIP) technologies is monitored	Is VoIP usage being monitored?	Review VoIP usage logs for anomalies - unusual call volumes, calls to unexpected destinations, or access from unexpected devices. Integrate VoIP logs with your SIEM if your platform supports it.
SC.L2-3.13.15	**[a]**	The authenticity of communications sessions is protected	When communicating over a network, do you verify the other party is actually who they claim to be?	Use TLS with valid certificates for web and API communications, VPN for remote connections, and mutual authentication where feasible. Certificate management processes ensure certificates remain valid, trusted, and not expired.
SC.L2-3.13.16	**[a]**	The confidentiality of CUI at rest is protected	Is sensitive data stored on your servers, drives, or in the cloud protected - or is it just sitting there exposed?	Encrypt CUI stored on servers, endpoints, and cloud storage. Combine encryption with access controls so that system access does not mean open access to all CUI. Virtru provides data-centric protection that stays with files regardless of where they are stored or shared.

System and Information Integrity (SI)

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SI.L2-3.14.1	**[a]**	The time within which to identify system flaws is specified	Have you set a timeframe for how quickly system vulnerabilities must be identified after they are discovered?	Define SLAs for flaw identification in your vulnerability management policy - for example, critical vulnerabilities identified within 24 hours of a scan completing or an advisory being published.
SI.L2-3.14.1	**[b]**	System flaws are identified within the specified time frame	Are vulnerabilities actually being identified within that timeframe?	Configure your vulnerability scanner to run on schedule and route results to your ticketing or vulnerability management platform automatically. Consistent, scheduled scanning is what makes identification timelines achievable.
SI.L2-3.14.1	**[c]**	The time within which to report system flaws is specified	Have you set a timeframe for how quickly identified vulnerabilities must be reported internally?	Define reporting timelines in your policy - for example, identified vulnerabilities reported to security leadership within 48 hours of discovery. Specify the reporting path, format, and who is responsible for initiating it.
SI.L2-3.14.1	**[d]**	System flaws are reported within the specified time frame	Are vulnerabilities actually being reported within that timeframe?	Configure automated notifications from your vulnerability scanner or ticketing platform to route findings to the appropriate people within the defined timeframe. Track notification compliance as a measurable metric.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SI.L2-3.14.1	**[e]**	The time within which to correct system flaws is specified	Have you set a timeframe for how quickly vulnerabilities must be corrected?	Define remediation SLAs by severity - for example, critical in 15 days, high in 30 days, medium in 90 days. Document these timelines in your policy and use them to drive your patch management program cadence.
SI.L2-3.14.1	**[f]**	System flaws are corrected within the specified time frame	Are vulnerabilities actually being fixed within that timeframe - not just acknowledged and left open?	Track remediation compliance in your vulnerability management platform or ticketing system. Vulnerabilities past their SLA should trigger escalation. Document formal risk acceptance with sign-off when timelines cannot be met.
SI.L2-3.14.2	**[a]**	Designated locations for malicious code protection are identified	Have you identified where malware protection needs to be deployed - workstations, servers, email gateways?	Conduct a coverage assessment to identify every location where malware protection is needed - workstations, servers, email gateways, web proxies, and any other entry points for malicious content entering your environment.
SI.L2-3.14.2	**[b]**	Protection from malicious code at designated locations is provided	Is malware protection actually deployed and running at those locations?	Deploy and verify endpoint protection at every identified location. Confirm agents are active, reporting, and not excluded from key directories or processes. Missing coverage on even a few systems is a significant gap.
SI.L2-3.14.3	**[a]**	Response actions to system security alerts and advisories are identified	Have you defined what actions to take when security alerts or advisories come in from vendors or CISA?	Define response actions for different types of alerts and advisories - some require immediate patching, others a risk assessment, others a compensating control. Document this decision framework in your security operations procedures.
SI.L2-3.14.3	**[b]**	System security alerts and advisories are monitored	Are you actively monitoring for security alerts and advisories relevant to your environment?	Subscribe to CISA's Known Exploited Vulnerabilities catalog, vendor security bulletins, and US-CERT advisories. Route these into a workflow where a specific person is responsible for reviewing and acting on them.
SI.L2-3.14.3	**[c]**	Actions in response to system security alerts and advisories are taken	When relevant alerts come in, are those defined response actions actually being taken?	Follow through on defined response actions when alerts come in. Log what was received, what decision was made, and what action was taken. An inbox full of unread security advisories is not a defense during an assessment.
SI.L2-3.14.4	**[a]**	Malicious code protection mechanisms are updated when new releases are available	Are malware protection tools updated automatically when new signatures or versions become available?	Configure antivirus and EDR tools to update signature databases automatically when new releases are available. Do not rely on manual updates. Audit the auto-update configuration periodically to confirm it is actually working.
SI.L2-3.14.5	**[a]**	The frequency for malicious code scans is defined	Have you defined how often malware scans must run on your systems?	Define scan frequency in your policy - daily scans for critical systems, weekly for others is a common approach. The frequency should be specific and defensible based on your risk profile and system criticality.

Control	Objective	CMMC Assessment Language	What It Means	How to Address It
SI.L2-3.14.5	**[b]**	Malicious code scans are performed with the defined frequency	Are those scans actually running on schedule?	Configure your endpoint protection to run scheduled scans at the defined frequency. Collect scan completion reports as evidence of compliance. Flag systems that miss scheduled scans for follow-up and investigation.
SI.L2-3.14.5	**[c]**	Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed	Are files downloaded from outside your organization scanned in real time as they are received, opened, or executed?	Enable real-time scanning for all files downloaded from the internet or received from external sources. This is typically a default setting in modern endpoint protection - verify it is enabled and not excluded for any file types or directories.
SI.L2-3.14.6	**[a]**	The system is monitored to detect attacks and indicators of potential attacks	Are your systems actively monitored to detect attacks or early signs that an attack is building?	Deploy IDS/IPS at network entry and exit points and feed alerts into your SIEM. Define which alert categories require human review. Someone needs to actually look at the alerts - not just collect them in a system.
SI.L2-3.14.6	**[b]**	Inbound communications traffic is monitored to detect attacks and indicators of potential attacks	Is incoming network traffic being monitored for attack indicators?	Monitor inbound traffic through your perimeter firewall, IDS/IPS, and email security gateway. Log all inbound connections and route suspicious patterns to your SIEM for correlation and triage.
SI.L2-3.14.6	**[c]**	Outbound communications traffic is monitored to detect attacks and indicators of potential attacks	Is outgoing traffic also being watched - unusual outbound activity can be an early sign of a breach?	Outbound monitoring is equally important and often overlooked. Unusual outbound connections can indicate data exfiltration or command-and-control activity. Configure your firewall and SIEM to flag outbound anomalies.
SI.L2-3.14.7	**[a]**	Authorized use of the system is defined	Have you defined what normal, authorized use of your systems looks like?	Document what authorized use of your systems looks like in your acceptable use policy. Be specific enough that unauthorized use has a clear definition - bulk data downloads, access without a business need, or use of unapproved external services.
SI.L2-3.14.7	**[b]**	The system is monitored to detect the unauthorized use of organizational systems	Do you have tools or processes in place to detect when your systems are being used in unauthorized ways?	Deploy SIEM, DLP, EDR, and user activity monitoring to detect violations. Define alert thresholds for anomalies like access at unusual hours, large file movements, or access to sensitive resources by unexpected user accounts.