CMMC COMPLIANCE WORKBOOK SERIES

WORKBOOK 3

Level 2 Gap Assessment

NIST SP 800-171 Rev 2 Implementation Guide
for Small Defense Contractors

Applies To:	All DoD contractors handling Controlled Unclassified Information (CUI)
Controls Covered:	110 controls — NIST SP 800-171 Rev 2 across 14 control families
Assessment Types:	Level 2 Self-Assessment OR Level 2 C3PAO Third-Party Assessment
POA&Ms; Allowed:	YES — but all items must close within 180 days of conditional status
Companion Docs:	WB4 (SSP Starter) | WB5 (POA&M; Tracker & SPRS Calculator)
Phase 2 Deadline:	November 10, 2026 — C3PAO certification required for most CUI contracts
Version:	1.0 • March 2026

■ LEGAL DISCLAIMER — READ BEFORE PROCEEDING

This workbook is an educational and self-assessment tool. It does not constitute legal advice, cybersecurity consulting, or a guarantee of CMMC compliance. False certifications submitted to DoD may expose organizations and senior officials to False Claims Act (FCA) liability, including damages up to three times the value of the affected contract. Consult qualified legal counsel before submitting any compliance certification to the DoD.

HOW TO USE THIS WORKBOOK

Purpose

This workbook guides you through a structured gap assessment against all 110 NIST SP 800-171 Rev 2 controls required for CMMC Level 2. Each control gets its own page with the verbatim requirement, plain-English translation, action steps, solutions, evidence checklist, and an interactive gap assessment status field. Use the companion Excel tracker (WB3_CMMC_Level2_Tracker.xlsx) to document your assessment, track gaps, and build your Plan of Action & Milestones (POA&M;).

Step 1	Read Section 1 to understand Level 2 scope and the CUI boundary assessment.
Step 2	Open the companion Excel tracker (WB3_CMMC_Level2_Tracker.xlsx) to your family tab.
Step 3	Work through each control page. Read, assess your current state, then mark Met / Partially Met / Not Met.
Step 4	For any Partially Met or Not Met control, document the gap and corrective action in the Excel tracker.
Step 5	Create a POA&M; entry in WB5 for every Not Met or Partially Met control.
Step 6	Review the Gap Summary Matrix (Section 2) to see your overall posture by control family.
Step 7	Once all gaps are remediated, complete the SSP (WB4) and submit your score to SPRS.

■ Understanding SPRS Weights

Each control carries a point weight used to calculate your SPRS score. Starting from 110, each unimplemented control is subtracted. Weights: –5 points (highest risk), –3 points (medium risk), –1 point (lower risk). The weight is shown in the top-right of each control page. Use WB5 (POA&M; Tracker & SPRS Calculator) to calculate your score at any time.

■ POA&Ms; Are Allowed at Level 2

Unlike Level 1, CMMC Level 2 permits a Plan of Action & Milestones (POA&M;) for controls that are not yet fully implemented. This allows a conditional CMMC status while you remediate gaps. However, all POA&M; items must be closed within 180 days of receiving conditional status. Track POA&M; items in WB5.

SECTION 1 | Understanding Your Level 2 Scope

1.1 The CUI Boundary

Your Level 2 assessment covers all systems, components, and locations within your **CUI boundary** — the set of assets that process, store, or transmit Controlled Unclassified Information (CUI). Defining this boundary accurately is critical: too narrow and you leave gaps; too broad and the assessment scope becomes unmanageable.

Asset Category	Definition & Scope Treatment
CUI Assets	Systems, components, and users that process, store, or transmit CUI. These are fully in scope and all 110 controls apply.
Security Protection Assets	Systems that provide security functions for the CUI environment (firewalls, SIEM, authentication servers). These must also meet all applicable controls.
Contractor Risk Managed Assets	Systems that can connect to CUI assets but do not process CUI. You manage risk through access controls and network segmentation.
Specialized Assets	Systems with unique constraints (IoT, OT, test equipment) that cannot fully meet all controls. Document and manage residual risk.
Out-of-Scope Assets	Systems with no connection to CUI and no ability to impact the CUI environment. Document why they are excluded from scope.

■ Document Your CUI Boundary Before Starting

Create a network diagram and asset inventory defining your CUI boundary before beginning this gap assessment. Use the Asset Inventory tab in WB3_CMMC_Level2_Tracker.xlsx. Your boundary definition should be captured in Section 2 of your SSP (WB4).

SECTION 2 | Gap Summary Matrix

Complete this summary matrix as you work through each control family. It provides a one-page view of your compliance posture across all 14 control families. This matrix should be updated and reviewed at each assessment cycle.

Family	Controls	Met	Partial	Not Met	% Met	SPRS Impact
AC Access Control	22					
AT Awareness & Training	3					
AU Audit & Accountability	9					
CA Assessment, Authorization & Monitoring	4					
CM Configuration Management	9					
IA Identification & Authentication	11					
IR Incident Response	3					
MA Maintenance	6					
MP Media Protection	9					
PE Physical Protection	6					
PS Personnel Security	2					
RA Risk Assessment	3					
SC System & Comm. Protection	16					
SI System & Info. Integrity	7					

TOTAL	**110**					

AC

Access Control

22 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
AC.L2-3.1.1	Authorized Access Control	**–5 pts**	Met Partial Not Met
AC.L2-3.1.2	Transaction & Function Control	**–3 pts**	Met Partial Not Met
AC.L2-3.1.3	Control CUI Flow	**–3 pts**	Met Partial Not Met
AC.L2-3.1.4	Separation of Duties	**–3 pts**	Met Partial Not Met
AC.L2-3.1.5	Least Privilege	**–3 pts**	Met Partial Not Met
AC.L2-3.1.6	Non-Privileged Account Use	**–3 pts**	Met Partial Not Met
AC.L2-3.1.7	Privileged Functions	**–3 pts**	Met Partial Not Met
AC.L2-3.1.8	Unsuccessful Logon Attempts	**–3 pts**	Met Partial Not Met
AC.L2-3.1.9	System Use Notification	**–1 pts**	Met Partial Not Met

AC.L2-3.1.10	Session Lock	**–1 pts**	Met Partial Not Met
AC.L2-3.1.11	Session Termination	**–1 pts**	Met Partial Not Met
AC.L2-3.1.12	Control Remote Access	**–3 pts**	Met Partial Not Met
AC.L2-3.1.13	Remote Access Confidentiality	**–3 pts**	Met Partial Not Met
AC.L2-3.1.14	Remote Access Routing	**–3 pts**	Met Partial Not Met
AC.L2-3.1.15	Privileged Remote Access	**–3 pts**	Met Partial Not Met
AC.L2-3.1.16	Wireless Access Authorization	**–1 pts**	Met Partial Not Met
AC.L2-3.1.17	Wireless Access Protection	**–1 pts**	Met Partial Not Met
AC.L2-3.1.18	Mobile Device Access Control	**–3 pts**	Met Partial Not Met
AC.L2-3.1.19	Encrypt CUI on Mobile	**–3 pts**	Met Partial Not Met
AC.L2-3.1.20	External System Connections	**–3 pts**	Met Partial Not Met
AC.L2-3.1.21	Portable Storage Use	**–3 pts**	Met Partial Not Met

AC.L2-3.1.22	Control CUI Posted to Websites	**–1 pts**	Met Partial Not Met

AC.L2-3.1.1

Access Control
Authorized Access Control

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

"Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems)."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Only authorized people, programs, and devices may access your systems. Maintain a current list of who has access and remove it immediately when no longer needed.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Maintain a current authorized user list for all CUI systems. 2. Disable accounts within 24 hours of employee departure or role change. 3. Inventory all authorized devices on your network. 4. Review access lists at least quarterly. 5. Document in your System Security Plan (SSP).	Active Directory or Azure AD. Microsoft 365 user management. Network access control solutions.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Current authorized user list with review dates.
- ■ Evidence of timely account disabling.
- ■ Device inventory showing authorized devices.
- ■ Access control policy in SSP.

Assessor Notes

Foundation of all access control. A current, accurate user list is the most common Level 2 assessment gap.

Your Notes:

AC.L2-3.1.2

Access Control
Transaction & Function Control

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Users should only be able to perform the actions their job requires. Implement role-based access controls so each user has the minimum permissions needed.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Define roles and assign least-privilege permissions. 2. Restrict admin rights to designated personnel only. 3. Prevent standard users from installing software. 4. Review role assignments annually. 5. Document in SSP.	Windows file/folder permissions. Active Directory groups and GPOs. Microsoft 365 role assignments.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Role-based access matrix showing permissions per role.
- Evidence admin rights are restricted.
- GPO or permission screenshots.
- Annual access review records.

Assessor Notes

Closely paired with AC.L2-3.1.1 — controls who logs in and what they can do.

Your Notes:

AC.L2-3.1.3 Access Control
Control CUI Flow

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Control the flow of CUI in accordance with approved authorizations."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

CUI must only move between authorized systems and people. You must have controls preventing CUI from flowing to unauthorized destinations — including unauthorized email, USB drives, or external systems.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Identify all authorized CUI pathways. 2. Block unauthorized CUI transfers using DLP or policy controls. 3. Prevent CUI from being sent to personal email. 4. Document approved CUI flow paths in SSP. 5. Train employees on approved CUI handling.	Microsoft Purview Information Protection (DLP). Email rules blocking personal email domains. USB blocking via Group Policy.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ Data flow diagram showing approved CUI pathways.
■ DLP policy configuration or equivalent.
■ Evidence unauthorized transfers are blocked.
■ SSP CUI flow documentation.

■ Assessor Notes

CUI data flow documentation is one of the most common assessment gaps — many organizations cannot produce a data flow diagram.

Your Notes:

AC.L2-3.1.4 Access Control
Separation of Duties

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

No single person should control all aspects of a critical process. Split sensitive tasks so fraud or error requires two people to collude.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Identify critical functions requiring separation. 2. Ensure no one person can both administer systems and review their own audit logs. 3. Separate financial approval and payment functions. 4. Document separation assignments in SSP.	Separate admin and auditor accounts in Active Directory. Multi-person approval workflows in Microsoft 365.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Documentation showing critical duties are separated across personnel.
- ■ Evidence no single account has both admin and audit review rights.
- ■ SSP section on separation of duties.

■ Assessor Notes

In small businesses, at minimum ensure no one person can make and approve critical system changes without oversight.

Your Notes:

AC.L2-3.1.5 Access Control
Least Privilege

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ enter here

Assessor: ■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Give users and processes only the minimum access required for their job. Privileged accounts should be separate from regular accounts and used only when necessary.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Create separate admin accounts for IT staff — use regular accounts for daily work. 2. Audit privileged account usage regularly. 3. Remove unnecessary privileges from all accounts. 4. Implement just-in-time admin access where possible. 5. Document least privilege policy in SSP.	Separate admin accounts in AD. Microsoft Privileged Identity Management (PIM) for Azure AD. Regular access reviews.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ List of privileged accounts with justification.
- ■ Evidence admin accounts are separate from daily-use accounts.
- ■ Privileged account usage audit logs.

■ Assessor Notes

One of the highest-impact controls — compromised admin accounts cause far more damage than compromised user accounts.

Your Notes:

AC.L2-3.1.6

Access Control
Non-Privileged Account Use

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Use non-privileged accounts or roles when accessing non-security functions."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

IT administrators must use their regular (non-admin) accounts for everyday tasks like email and browsing. Admin accounts should only be used when elevated privileges are actually required.

WHAT YOU NEED TO DO

1. Ensure all IT staff have separate regular user accounts for daily work.
2. Train IT staff on when to use admin vs. standard accounts.
3. Configure admin accounts without email or browser access.
4. Audit logon events for admin accounts used during non-admin activities.

COMMON SMALL BUSINESS SOLUTIONS

Separate AD accounts for admin vs. standard use. Browser and email profiles tied to standard accounts only.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Evidence that admin accounts are distinct from daily-use accounts.
- ■ Logon audit logs showing appropriate account usage.
- ■ Policy documentation on account separation.

■ Assessor Notes

Closely related to AC.L2-3.1.5 — together these require separate accounts and restricted use of admin accounts.

Your Notes:

AC.L2-3.1.7 Access Control Privileged Functions

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Regular users must not be able to perform administrative actions. All privileged function executions must be logged so you can detect and investigate misuse.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Configure systems so non-admin users cannot execute privileged functions. 2. Enable audit logging for all privileged function executions. 3. Review privileged function audit logs regularly. 4. Alert on unexpected privileged function use.	Windows Event Logs (Security log). SIEM tools. Group Policy to restrict privileged functions. Microsoft Sentinel.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ System configuration showing non-privileged users cannot execute privileged functions.
- ■ Audit log samples showing privileged function capture.
- ■ Log review records.

■ Assessor Notes

The audit logging requirement here connects directly to AU (Audit & Accountability) controls.

Your Notes:

AC.L2-3.1.8 Access Control
Unsuccessful Logon Attempts

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Limit unsuccessful logon attempts."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ enter here

Assessor: ■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Lock accounts or introduce delays after repeated failed login attempts. This prevents brute force password attacks.

WHAT YOU NEED TO DO

1. Configure account lockout after 5-10 failed attempts.
2. Set lockout duration to at least 15 minutes.
3. Alert on excessive failed login attempts.
4. Apply to all systems including VPN, email, and remote access.
5. Document lockout policy in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Windows Account Lockout Policy via Group Policy. Microsoft 365 Smart Lockout. Azure AD Conditional Access.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Account lockout policy configuration.
- ■ Evidence policy is applied to all in-scope systems.
- ■ Alert configuration for excessive failed attempts.

■ Assessor Notes

One of the easiest controls to implement — Group Policy account lockout takes minutes to configure.

Your Notes:

AC.L2-3.1.9	Access Control System Use Notification	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Provide privacy and security notices consistent with CUI rules."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Display a warning banner when users log into any CUI system. The banner must inform users that activity may be monitored and unauthorized use is prohibited.

WHAT YOU NEED TO DO

1. Configure login banners on all systems (Windows, servers, VPN, remote access).
2. Banner must reference CUI handling and monitoring.
3. Banner must require user acknowledgment before proceeding.
4. Test all entry points to ensure banner displays.
5. Document banner text in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Windows Group Policy: Computer Configuration → Security Settings → Local Policies → Interactive logon message. VPN and remote access login banners.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Screenshots of login banners on all in-scope systems.
- ■ Banner text meeting CUI notification requirements.
- ■ GPO configuration showing banner is enforced.

Assessor Notes

Sample DoD-approved banner: 'You are accessing a U.S. Government information system... Unauthorized use is prohibited and subject to criminal and civil penalties.'

Your Notes:

AC.L2-3.1.10	Access Control Session Lock	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Use session lock with pattern-hiding displays after a period of inactivity."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Systems must automatically lock after inactivity and display a pattern hiding screen content. Users must re-authenticate to unlock.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Configure screen lock after 15 minutes of inactivity on all systems. 2. Require password to unlock screensaver. 3. Apply to all desktops, laptops, and remote sessions. 4. Enforce via Group Policy to prevent users from disabling it.	Windows Group Policy: Screen saver + password protect + idle timeout. Microsoft Intune for mobile/remote devices.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ Group Policy configuration showing session lock settings.
■ Screenshots confirming lock is applied on all systems.
■ Evidence that users cannot disable the lock.

■ Assessor Notes

Very common gap — employees often disable screensaver locks for convenience. Enforce via GPO.

Your Notes:

AC.L2-3.1.11	Access Control Session Termination	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Beyond session locking, certain sessions should be fully terminated under defined conditions such as after extended inactivity or at the end of a work period.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Define conditions for session termination (e.g., 4+ hours inactivity, end of workday). 2. Configure automatic termination for remote access sessions. 3. Apply to web-based CUI applications. 4. Document termination conditions in SSP.	Windows Group Policy: Force logoff after idle time. Remote Desktop Session Host timeout. VPN session timeout. Microsoft 365 session policies.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Session termination policy documentation.
- ■ Remote access session timeout configuration.
- ■ SSP section defining termination conditions.

■ Assessor Notes

Most important for remote/VPN sessions. A forgotten open VPN session is a significant risk.

Your Notes:

AC.L2-3.1.12	Access Control Control Remote Access	SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Monitor and control remote access sessions."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Remote access (VPN, RDP, remote support tools) must be monitored, controlled, and logged. Know who is connected remotely at all times.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Use VPN for all remote access to internal systems. 2. Log all remote access sessions (who, when, from where, duration). 3. Disable split tunneling on VPN. 4. Review remote access logs regularly. 5. Terminate inactive remote sessions automatically.	Business-grade VPN (Cisco AnyConnect, GlobalProtect, WireGuard). Disable RDP direct to internet. Use jump servers or bastion hosts.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ VPN configuration documentation.
■ Remote access session logs.
■ Evidence that direct RDP from internet is blocked.
■ Split tunneling configuration (disabled).

Assessor Notes

Direct RDP exposure to the internet is one of the most common attack vectors. Never allow RDP direct from internet.

Your Notes:

AC.L2-3.1.13 Access Control
Remote Access Confidentiality

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

All remote connections must be encrypted. Unencrypted remote access protocols (Telnet, plain FTP) are prohibited for CUI systems.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Ensure all remote access uses encrypted protocols (TLS 1.2+, SSH, IPsec VPN). 2. Disable unencrypted remote access protocols (Telnet, FTP, HTTP). 3. Verify VPN uses strong encryption (AES-256). 4. Scan for and remediate any unencrypted remote services.	TLS 1.2 or higher. IPsec or SSL/TLS VPN. SSH for server management. FIPS 140-2 validated encryption where required.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ VPN encryption configuration (algorithm, key length).
- ■ Evidence that unencrypted protocols are disabled.
- ■ Network scan results showing no unencrypted remote services.

■ Assessor Notes

All remote access must use FIPS-validated cryptography for contracts requiring it.

Your Notes:

AC.L2-3.1.14 Access Control
Remote Access Routing

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Route remote access via managed access control points."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Remote access traffic must pass through a controlled gateway — not connect directly peer-to-peer to internal systems.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Ensure all remote access goes through your VPN gateway. 2. Block direct external access to internal systems bypassing VPN. 3. Use network segmentation to prevent direct remote access to CUI systems. 4. Monitor all managed access points.	VPN gateway as single entry point. Firewall rules blocking direct external access. Zero Trust Network Access (ZTNA) solutions.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Network diagram showing remote access routing through managed access points.
- Firewall rules blocking direct external access.
- VPN gateway configuration.

Assessor Notes

Prevents attackers from establishing direct connections that bypass your security controls.

Your Notes:

AC.L2-3.1.15 Access Control
Privileged Remote Access

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Authorize remote execution of privileged commands and remote access to security-relevant information via remote access only for documented operational needs."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Running admin commands remotely must be explicitly authorized and documented. Remote privileged access should be limited to documented operational needs only.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Document all approved use cases for remote privileged access. 2. Require additional authentication for remote privileged sessions. 3. Log all remote privileged command execution. 4. Limit remote privileged access to specific personnel and systems.	Privileged Access Management (PAM) solutions. Just-in-time admin access. Enhanced logging for privileged remote sessions.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Documentation of approved remote privileged access use cases.
- ■ Enhanced authentication configuration for privileged remote access.
- ■ Privileged remote access session logs.

■ Assessor Notes

High-value target — compromised privileged remote access gives attackers full system control.

Your Notes:

AC.L2-3.1.16	Access Control Wireless Access Authorization	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Authorize wireless access prior to allowing such connections."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Wireless connections must be explicitly authorized before they are allowed. No unauthorized devices should connect to your wireless network.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Maintain a list of all authorized wireless devices. 2. Use WPA3 or WPA2-Enterprise for wireless authentication. 3. Implement MAC address filtering as a supplementary control. 4. Scan for and disable unauthorized wireless access points.	WPA2-Enterprise with 802.1X authentication. Microsoft NPS (RADIUS server). Network Access Control (NAC). Rogue AP detection.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Authorized wireless device list.
- ■ Wireless authentication configuration (WPA2-Enterprise or WPA3).
- ■ Periodic wireless access review records.
- ■ Rogue AP detection evidence.

■ Assessor Notes

WPA2-Personal (shared password) is insufficient for CUI environments. Implement WPA2-Enterprise.

Your Notes:

AC.L2-3.1.17	Access Control Wireless Access Protection	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Protect wireless access using authentication and encryption."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Protect wireless connections with strong authentication and encryption to prevent eavesdropping.

WHAT YOU NEED TO DO

1. Configure all wireless networks with WPA2 or WPA3 encryption.
2. Use enterprise authentication (802.1X) not shared passwords.
3. Change encryption keys when personnel with access depart.
4. Separate guest wireless from business wireless.

COMMON SMALL BUSINESS SOLUTIONS

WPA3 (preferred) or WPA2-Enterprise. RADIUS authentication. Separate SSIDs for guest and business.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Wireless encryption configuration screenshots.
- ■ Evidence of enterprise authentication.
- ■ Guest network separation configuration.

■ Assessor Notes

Many small businesses use WPA2-Personal (shared password) — this does not meet Level 2 requirements.

Your Notes:

AC.L2-3.1.18	Access Control Mobile Device Access Control	SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Control connection of mobile devices."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Mobile devices accessing CUI must be managed and controlled. Unmanaged personal devices should not access CUI.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Implement Mobile Device Management (MDM) for all CUI-accessing devices. 2. Require MDM enrollment before allowing mobile access. 3. Enforce minimum security requirements (PIN, encryption, remote wipe). 4. Block access from unmanaged devices.	Microsoft Intune (MDM). Apple Business Manager. Android Enterprise. Conditional Access blocking unmanaged devices.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ MDM enrollment records for all authorized mobile devices.
■ MDM policy configuration.
■ Evidence that unmanaged devices are blocked.
■ Conditional Access policy configuration.

■ Assessor Notes

Personal phones used to check work email are a major compliance gap. MDM enrollment is required.

Your Notes:

AC.L2-3.1.19 Access Control
Encrypt CUI on Mobile

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Encrypt CUI on mobile devices and mobile computing platforms."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

CUI stored on mobile devices must be encrypted — phones, tablets, and laptops used outside the office.

WHAT YOU NEED TO DO

1. Enable full-disk encryption on all laptops (BitLocker for Windows, FileVault for Mac).
2. Enable device encryption on all smartphones and tablets.
3. Verify encryption via MDM compliance policies.
4. Document encryption requirements in mobile device policy.

COMMON SMALL BUSINESS SOLUTIONS

BitLocker (Windows — free, built-in). FileVault (Mac — free, built-in). iOS and Android encrypt by default when a PIN is set. MDM compliance reporting.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ BitLocker/FileVault status on all laptops.
- ■ MDM compliance report showing mobile encryption status.
- ■ Mobile device encryption policy.

■ Assessor Notes

BitLocker is free and built into Windows Pro/Enterprise. Enable it on all laptops — one of the highest-value easy wins.

Your Notes:

AC.L2-3.1.20

Access Control
External System Connections

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Verify and control/limit connections to external systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Control connections between your systems and external systems (vendors, partners, cloud services). Each connection that can access CUI must be authorized and controlled.

WHAT YOU NEED TO DO

1. Inventory all connections to external systems that can access CUI.
2. Establish formal agreements (ISAs, MOUs) with external system owners.
3. Apply access controls on all external connections.
4. Review external system connections annually.
5. Document in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Formal Interconnection Security Agreements (ISAs). Network segmentation for external access. VPN tunnels to partner systems. Cloud service security reviews.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Inventory of all external system connections.
- Interconnection agreements for each connection.
- Access control configuration for external connections.
- Annual review records.

Assessor Notes

Cloud services, MSP access, and partner connections are all external system connections requiring documentation.

Your Notes:

AC.L2-3.1.21 Access Control
Portable Storage Use

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Limit use of portable storage devices on external systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Control USB drive use on your systems. Limit what devices can be connected and log usage.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Block or restrict USB storage via Group Policy. 2. Allow only approved/encrypted USB devices. 3. Log USB device connection events. 4. Implement a formal removable media policy.	Group Policy: Computer Configuration → Removable Storage Access. BitLocker To Go for USB encryption. Device control solutions.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Group Policy configuration restricting USB storage.
- ■ Approved device list if using whitelist approach.
- ■ USB connection audit logs.
- ■ Removable media policy.

■ Assessor Notes

USB drives are one of the easiest ways to exfiltrate CUI. At minimum, enforce encrypted USB only and log all connections.

Your Notes:

AC.L2-3.1.22

Access Control
Control CUI Posted to Websites

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Control CUI posted or processed on publicly accessible systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Do not post CUI on public-facing websites. Ensure content on public systems is reviewed before publication.

WHAT YOU NEED TO DO

1. Establish a review process for all content posted to public websites.
2. Train employees on CUI prohibition on public posting.
3. Scan public-facing systems periodically for CUI.
4. Implement content review workflows for web publishing.

COMMON SMALL BUSINESS SOLUTIONS

Content management system approval workflows. DLP scanning of public content. Employee CUI training. Periodic manual review.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Content review/approval process documentation.
- ■ Training records on CUI handling.
- ■ Evidence of periodic scans of public content.
- ■ Policy prohibiting CUI on public systems.

■ Assessor Notes

One inadvertently posted document with CUI markings is a reportable incident.

Your Notes:

A T

Awareness & Training

3 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
AT.L2-3.2.1	Literacy Training and Awareness	**–3 pts**	Met Partial Not Met
AT.L2-3.2.2	Role-Based Training	**–3 pts**	Met Partial Not Met
AT.L2-3.2.3	Insider Threat Awareness	**–3 pts**	Met Partial Not Met

AT.L2-3.2.1

Awareness & Training
Literacy Training and Awareness

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

All employees who use CUI systems must receive security awareness training annually covering risks, policies, and personal responsibilities.

WHAT YOU NEED TO DO

1. Conduct security awareness training for all staff at least annually.
2. Cover CUI handling, phishing, password security, and incident reporting.
3. Document training completion for each employee.
4. Include new hire training within 30 days of start.
5. Update content when threats or policies change.

COMMON SMALL BUSINESS SOLUTIONS

KnowBe4, Proofpoint Security Awareness, SANS Security Awareness. DoD Cyber Awareness Challenge (free — public.cyber.mil). Track completions in WB3 tracker.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Training completion records for all employees.
- ■ Training curriculum documentation.
- ■ New hire training policy.
- ■ Annual training schedule.

Assessor Notes

The free DoD Cyber Awareness Challenge (public.cyber.mil) satisfies this control for most small businesses.

Your Notes:

AT.L2-3.2.2

Awareness & Training
Role-Based Training

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Ensure that individuals performing assigned security-related duties are adequately trained to carry out their assigned information security-related duties and responsibilities."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Personnel with specific security responsibilities (IT staff, system administrators, security officers) must receive role-specific training beyond general awareness.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Identify all personnel with security-related duties. 2. Provide role-specific training for IT administrators and security officers. 3. Document role-based training requirements and completions. 4. Include vendor/contractor security training requirements in contracts.	SANS Institute courses. CompTIA Security+/CySA+ certifications. Vendor-specific training. NIST NICE framework resources.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Role-specific training curriculum per security role.
- ■ Training completion records by role.
- ■ Documentation of training requirements for each security role.

■ Assessor Notes

IT administrators managing CUI systems need technical security training relevant to their specific tools and responsibilities.

Your Notes:

AT.L2-3.2.3	Awareness & Training Insider Threat Awareness	SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Train employees to recognize and report signs of insider threats — colleagues showing warning signs of malicious intent or accidental data exposure.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Include insider threat recognition in annual security training. 2. Train employees on reporting procedures. 3. Cover behavioral indicators of insider threat. 4. Establish confidential reporting mechanisms.	CISA insider threat awareness resources (free). CERT Insider Threat Center resources. Include as a module in existing awareness training platform.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Training content covering insider threat indicators.
- ■ Training completion records.
- ■ Reporting procedure documentation.

■ Assessor Notes

The definition of 'insider threat' includes both malicious insiders and well-meaning employees who accidentally expose CUI.

Your Notes:

AU Audit & Accountability

9 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
AU.L2-3.3.1	Event Logging	**–5 pts**	Met Partial Not Met
AU.L2-3.3.2	User Accountability	**–3 pts**	Met Partial Not Met
AU.L2-3.3.3	Event Review	**–3 pts**	Met Partial Not Met
AU.L2-3.3.4	Audit Failure Alerting	**–3 pts**	Met Partial Not Met
AU.L2-3.3.5	Audit Correlation	**–3 pts**	Met Partial Not Met
AU.L2-3.3.6	Reduction & Reporting	**–3 pts**	Met Partial Not Met
AU.L2-3.3.7	Authoritative Time Source	**–1 pts**	Met Partial Not Met
AU.L2-3.3.8	Audit Protection	**–3 pts**	Met Partial Not Met
AU.L2-3.3.9	Audit Management	**–3 pts**	Met Partial Not Met

AU.L2-3.3.1

Audit & Accountability
Event Logging

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ enter here

Assessor:
■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Log security-relevant events on all CUI systems and retain them long enough to support incident investigation.

WHAT YOU NEED TO DO

1. Enable audit logging on all systems (Windows Event Log, server logs, network device logs).
2. Log: logon/logoff, account management, privilege use, object access, policy changes.
3. Retain logs at least 90 days online, 1 year total.
4. Protect logs from unauthorized modification or deletion.

COMMON SMALL BUSINESS SOLUTIONS

Windows Event Log. Syslog for network devices. Microsoft Sentinel (SIEM). Centralized log management. Increase default Event Log sizes.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Audit logging configuration on all in-scope systems.
- ■ Log retention policy and configuration.
- ■ Sample audit logs showing required event categories.
- ■ Log protection configuration.

■ Assessor Notes

Windows default Event Log sizes overwrite quickly. Increase log sizes and implement archival immediately.

Your Notes:

AU.L2-3.3.2

Audit & Accountability
User Accountability

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Audit logs must tie specific actions to specific individual users. This requires unique accounts and logging that captures user identity.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Eliminate all shared accounts — each user must have a unique account. 2. Ensure audit logs capture user identity for all logged events. 3. Prevent users from disabling or clearing audit logs. 4. Implement user activity monitoring where appropriate.	Individual Windows accounts with audit logging. Microsoft 365 unified audit log. No shared accounts for interactive use.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Evidence that all accounts are individual (no shared accounts).
- ■ Audit log samples showing user identity captured.
- ■ Configuration preventing users from clearing logs.

■ Assessor Notes

Shared accounts make user accountability impossible — directly requires the individual user accounts from AC controls.

Your Notes:

AU.L2-3.3.3

Audit & Accountability
Event Review

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Review and update logged events."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Regularly review audit logs to detect suspicious activity and security incidents. Logs are only useful if someone reads them.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Define which events require review and how frequently. 2. Review security-relevant logs at least weekly. 3. Investigate and document anomalies detected. 4. Automate alerting for high-priority events.	Microsoft Sentinel automated alerting. Windows Event Viewer for manual review. SIEM solutions. Managed SOC services for small businesses.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Log review schedule and records showing regular review.
- Evidence of anomaly investigation.
- Alert configuration for critical events.
- Documented log review procedure.

Assessor Notes

The most common gap: logs collected but never reviewed. Automated alerting for critical events is essential.

Your Notes:

AU.L2-3.3.4

Audit & Accountability
Audit Failure Alerting

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Alert in the event of an audit logging process failure."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

If audit logging fails or stops recording events, you must be alerted immediately. Blind spots in logging are a security risk.

WHAT YOU NEED TO DO

1. Configure alerts for audit log failure or service stoppage.
2. Monitor log ingestion health in SIEM.
3. Test audit failure alerting regularly.
4. Document response procedure for audit failures.

COMMON SMALL BUSINESS SOLUTIONS

Windows Event Log service monitoring. SIEM health monitoring. Email alerts from log management system.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Alert configuration for audit logging failures.
- ■ Evidence of log health monitoring.
- ■ Test records showing alerts fire correctly.
- ■ Response procedure for audit failures.

■ Assessor Notes

Attackers who disable logging before an attack go undetected if you don't monitor for logging failures.

Your Notes:

AU.L2-3.3.5

Audit & Accountability
Audit Correlation

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Correlate events across multiple systems to detect and investigate incidents spanning multiple systems or time periods.

WHAT YOU NEED TO DO

1. Centralize logs from all systems into a SIEM or log management platform.
2. Configure correlation rules to detect multi-system attack patterns.
3. Establish incident investigation procedures using correlated logs.
4. Document correlation capabilities in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Microsoft Sentinel (SIEM with built-in correlation rules). Splunk. Even simple log aggregation improves correlation capability.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Centralized log management or SIEM configuration.
- ■ Correlation rule examples.
- ■ Incident investigation procedure referencing log correlation.
- ■ SSP section on audit correlation.

■ Assessor Notes

Even a basic centralized log server dramatically improves correlation over reviewing logs on individual systems.

Your Notes:

AU.L2-3.3.6

Audit & Accountability
Reduction & Reporting

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Your log management system must support filtering, reducing, and reporting on audit data to support investigations without analyzing every raw log entry.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Implement log filtering and search capability. 2. Create standard reports for common compliance needs. 3. Train staff on querying audit logs for investigation. 4. Document reporting capabilities.	SIEM query tools (Sentinel KQL, Splunk SPL). Log management search interfaces. Pre-built compliance reports. Windows Event Viewer filtering.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Evidence of log query/search capability.
- ■ Sample compliance reports or dashboards.
- ■ Documentation of reporting procedures.

■ Assessor Notes

The ability to answer 'show me all access by user X between dates A and B' is the minimum bar.

Your Notes:

AU.L2-3.3.7 Audit & Accountability
Authoritative Time Source

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

All systems must synchronize clocks to an authoritative NTP source. This ensures audit logs have accurate timestamps for incident investigation.

WHAT YOU NEED TO DO

1. Configure all systems to sync time via NTP (time.nist.gov or USNO).
2. Verify NTP synchronization regularly.
3. Use consistent time zones across all systems.
4. Monitor for time synchronization failures.

COMMON SMALL BUSINESS SOLUTIONS

Windows Time Service (W32tm) via Group Policy to use NIST/USNO NTP servers. Linux: timedatectl with NTP. Network device NTP configuration.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ NTP configuration on all systems.
- ■ Evidence of successful time synchronization.
- ■ Consistent timezone configuration across systems.

■ Assessor Notes

Time synchronization failures make log correlation impossible. Free and quick to fix via Group Policy.

Your Notes:

AU.L2-3.3.8

Audit & Accountability
Audit Protection

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Audit logs and collection tools must be protected. Users should not be able to delete or modify logs to cover their tracks.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Restrict access to audit logs to authorized personnel only. 2. Configure logs to be write-protected or append-only. 3. Send logs to a separate, protected log server. 4. Monitor for attempts to clear or modify logs.	Centralized log server with restricted access. Windows Event Log permissions. SIEM with immutable log storage. Azure Monitor immutable storage.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Access control configuration for audit log files.
- ■ Evidence logs are stored separately from monitored systems.
- ■ Log integrity monitoring configuration.
- ■ Evidence that log deletion generates an alert.

■ Assessor Notes

Sending logs to a separate system immediately makes them harder to tamper with — an architectural requirement.

Your Notes:

AU.L2-3.3.9

Audit & Accountability
Audit Management

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Only a limited set of authorized administrators should configure, manage, and maintain the audit logging system.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Designate specific personnel responsible for audit log management. 2. Restrict audit system configuration rights to designated personnel. 3. Separate audit administration from system administration. 4. Document audit management roles in SSP.	Dedicated audit administrator account separate from system admin. Role-based access in SIEM. Windows: Manage auditing and security log user right.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- List of personnel authorized to manage audit logging.
- Evidence that audit management rights are restricted.
- Role separation documentation.

Assessor Notes

The person administering systems should ideally not also control the audit logs for those systems — separation of duties.

Your Notes:

CA Assessment, Authorization & Monitoring

4 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
CA.L2-3.12.1	Security Assessment	**–3 pts**	Met Partial Not Met
CA.L2-3.12.2	Plan of Action	**–5 pts**	Met Partial Not Met
CA.L2-3.12.3	Security Control Monitoring	**–3 pts**	Met Partial Not Met
CA.L2-3.12.4	System Security Plan	**–5 pts**	Met Partial Not Met

CA.L2-3.12.1 Assessment, Authorization & Monitoring

Security Assessment

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:

■ *enter here*

Assessor:

■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Regularly test and evaluate whether your security controls are actually working. Don't just implement controls — verify they do what you think they do.

WHAT YOU NEED TO DO

1. Conduct an annual security control assessment of all CUI systems.
2. Test key controls for effectiveness.
3. Document assessment findings and remediate gaps.
4. Use results to update SSP and POA&M.;

COMMON SMALL BUSINESS SOLUTIONS

Annual self-assessment using CMMC Level 2 Assessment Guide. Vulnerability scanning tools (Tenable Nessus, Qualys). Penetration testing.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Annual security assessment report.
- ■ Testing evidence for key controls.
- ■ Remediation records for findings.
- ■ Updated SSP reflecting assessment results.

■ Assessor Notes

The self-assessment you are completing now satisfies this control for the current period. Document your assessment process.

Your Notes:

CA.L2-3.12.2 Assessment, Authorization & Monitoring

Plan of Action

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When you identify security gaps, document a formal Plan of Action & Milestones (POA&M;) to track each gap to closure.

WHAT YOU NEED TO DO

1. Create a POA&M; entry for every identified security control gap.
2. Each entry must include: control ID, gap description, corrective action, responsible party, resources, and completion date.
3. Review and update the POA&M; at least quarterly.
4. Close items within required timeframes.
5. Document the POA&M; in your SPRS submission.

COMMON SMALL BUSINESS SOLUTIONS

Use WB5 POA&M; tracker. SPRS POA&M; submission. Spreadsheet tracking gaps and remediation timelines.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Current POA&M; with all open items.
- ■ Evidence of quarterly POA&M; reviews.
- ■ Records of closed items with completion evidence.
- ■ POA&M; submitted to SPRS.

Assessor Notes

The POA&M; is a central compliance artifact. Level 2 allows POA&Ms; but all items must close within 180 days of conditional status.

Your Notes:

CA.L2-3.12.3

Assessment, Authorization & Monitoring
Security Control Monitoring

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Continuously verify that controls remain configured correctly and are working as intended.

WHAT YOU NEED TO DO

1. Implement continuous monitoring of key security controls.
2. Automate monitoring where possible.
3. Define monitoring frequency for each control category.
4. Document continuous monitoring strategy in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Vulnerability scanners (run monthly). Configuration compliance tools. Microsoft Secure Score. Windows Security Center monitoring.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Continuous monitoring plan in SSP.
- ■ Vulnerability scan schedules and recent results.
- ■ Configuration compliance scan results.
- ■ Evidence of regular monitoring activities.

■ Assessor Notes

Automation is key — manual monitoring of 110 controls is not sustainable. Prioritize automating critical controls.

Your Notes:

CA.L2-3.12.4

Assessment, Authorization & Monitoring
System Security Plan

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

The System Security Plan (SSP) is the master document describing your security posture. It must be comprehensive, current, and updated when systems change.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Develop a complete SSP covering all required sections (use WB4 template). 2. Include system boundary, CUI categories, user roles, external connections, and all 110 control implementations. 3. Review and update the SSP at least annually. 4. Update the SSP within 30 days of any significant system change.	WB4 SSP Starter template. NIST SP 800-18 SSP guidance. Document must describe ACTUAL implementation — not planned.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Completed SSP covering all required sections.
- ■ Evidence of annual SSP review.
- ■ Change management records showing SSP updates.
- ■ SSP approved by appropriate authority.

Assessor Notes

The SSP is the single most important document in your CMMC program. Inaccuracies are a leading cause of assessment failure.

Your Notes:

C
M

Configuration Management

9 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
CM.L2-3.4.1	Baseline Configurations	**–5 pts**	Met Partial Not Met
CM.L2-3.4.2	Security Configuration Enforcement	**–3 pts**	Met Partial Not Met
CM.L2-3.4.3	Change Control	**–3 pts**	Met Partial Not Met
CM.L2-3.4.4	Security Impact Analysis	**–3 pts**	Met Partial Not Met
CM.L2-3.4.5	Access Restrictions for Change	**–3 pts**	Met Partial Not Met
CM.L2-3.4.6	Least Functionality	**–3 pts**	Met Partial Not Met
CM.L2-3.4.7	Nonessential Programs	**–3 pts**	Met Partial Not Met
CM.L2-3.4.8	Application Execution Policy	**–5 pts**	Met Partial Not Met
CM.L2-3.4.9	User-Installed Software	**–3 pts**	Met Partial Not Met

CM.L2-3.4.1

Configuration Management
Baseline Configurations

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Define and document the standard, secure configuration for every system type. Maintain a complete inventory of all hardware and software.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Create documented baseline configurations for all system types. 2. Maintain complete hardware and software inventory. 3. Use CIS Benchmarks as starting point for baselines. 4. Update baselines when new systems are added or significant changes occur.	CIS Benchmarks (free at cisecurity.org). Microsoft Security Compliance Toolkit. DISA STIGs. Asset inventory tools (Lansweeper, Snipe-IT).

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Baseline configuration documentation for each system type.
- Hardware and software inventory.
- Evidence that CIS Benchmarks or equivalent are used.
- Process for updating baselines.

■ Assessor Notes

CIS Benchmarks provide free, ready-made baseline configurations for Windows, Linux, network devices, and cloud services.

Your Notes:

CM.L2-3.4.2

Configuration Management
Security Configuration Enforcement

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

After defining baselines, actively enforce them on all systems.

WHAT YOU NEED TO DO

1. Deploy baseline configurations via Group Policy or configuration management tools.
2. Scan regularly to detect configuration drift.
3. Remediate deviations within defined timeframes.
4. Document enforcement mechanism in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Windows Group Policy. Microsoft Intune. CIS-CAT tool (free) to assess CIS Benchmark compliance. PowerShell DSC.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Group Policy or config management deployment evidence.
- ■ Configuration compliance scan results.
- ■ Deviation remediation records.

■ Assessor Notes

Group Policy covers a large portion of this control for Windows environments. Base GPOs on CIS Benchmarks.

Your Notes:

CM.L2-3.4.3 Configuration Management Change Control

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Track, review, approve, and log changes to organizational systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

All changes to CUI systems must go through a formal change control process. Undocumented changes are a security and compliance risk.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Implement a change management process. 2. Require approval for all significant system changes. 3. Log all changes (who, when, why). 4. Include rollback procedures. 5. Review changes for security vulnerabilities.	IT service management tools (ServiceNow, Jira Service Management — some free tiers). Simple change log spreadsheet. SharePoint for approval workflows.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Change management policy or procedure.
- Change log showing recent changes with approvals.
- Evidence of security review for changes.
- Rollback procedure documentation.

Assessor Notes

For small businesses, even a simple spreadsheet tracking changes with approvals satisfies this control.

Your Notes:

CM.L2-3.4.4

Configuration Management
Security Impact Analysis

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Analyze the security impact of changes prior to implementation."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Before implementing system changes, assess how they might affect your security posture.

WHAT YOU NEED TO DO

1. Include security impact assessment as a required step in change management.
2. Evaluate changes against security baseline and known vulnerabilities.
3. Test changes in non-production before production deployment.
4. Document security impact assessments for significant changes.

COMMON SMALL BUSINESS SOLUTIONS

Pre-deployment security checklist. Test/staging environment. Vulnerability scan of changes before deployment. Peer review of configuration changes.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Security impact assessment records for significant changes.
- ■ Evidence of pre-production testing.
- ■ Change approval documentation referencing security assessment.

■ Assessor Notes

Even a simple checklist ('does this open new firewall ports? does this disable logging?') satisfies this control.

Your Notes:

CM.L2-3.4.5

Configuration Management
Access Restrictions for Change

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Limit who can make changes to your systems. Only authorized personnel should modify system configurations.

WHAT YOU NEED TO DO

1. Define who is authorized to make changes to each system type.
2. Restrict system configuration access to authorized change implementers.
3. Require separate authorization from implementation.
4. Document access restrictions in change management policy.

COMMON SMALL BUSINESS SOLUTIONS

Role-based access control for configuration management. Separate admin accounts for change implementation. Approval workflows in change management systems.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Access control configuration showing change rights are restricted.
- ■ Change authorization records showing approval before implementation.
- ■ Documentation of who is authorized to make changes.

■ Assessor Notes

The approver and implementer of changes should ideally be different people — separation of duties applied to change management.

Your Notes:

CM.L2-3.4.6

Configuration Management
Least Functionality

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Configure the organizational system to provide only essential capabilities."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Disable or remove unnecessary services, features, ports, and functions from all systems.

WHAT YOU NEED TO DO

1. Audit all running services and disable unnecessary ones.
2. Close unused network ports and protocols.
3. Remove unnecessary software and applications.
4. Disable unnecessary OS features (PowerShell v2, SMBv1, Telnet).
5. Document essential functions in baseline configuration.

COMMON SMALL BUSINESS SOLUTIONS

Windows Server Manager: disable unnecessary roles. Services.msc: disable unnecessary services. Firewall: close unused ports. CIS Benchmarks list specific services to disable.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Running services audit showing unnecessary services disabled.
- Open ports scan showing only necessary ports.
- Software inventory showing no unnecessary applications.
- Baseline configuration listing essential functions only.

Assessor Notes

SMBv1 (EternalBlue vulnerability) and PowerShell v2 (bypasses logging) should be disabled on all Windows systems immediately.

Your Notes:

CM.L2-3.4.7 Configuration Management Nonessential Programs

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Actively prevent unauthorized software and features from running on CUI systems.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Implement application whitelisting or application control. 2. Block execution of scripts from unauthorized locations. 3. Disable unused communication protocols. 4. Prevent installation of unauthorized software.	Windows Defender Application Control (WDAC — built-in). AppLocker (Windows Enterprise). Software Restriction Policies via Group Policy.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Application control policy configuration.
- Evidence that unauthorized software cannot execute.
- Protocol restriction configuration.

Assessor Notes

Group Policy software restriction policies and blocking script execution from user directories are achievable first steps.

Your Notes:

CM.L2-3.4.8	Configuration Management Application Execution Policy	SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

"Apply deny-by-default, allow-by-exception (whitelisting) policy to prevent the use of unauthorized software."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Implement a formal policy where software execution is denied by default and only explicitly approved applications are allowed to run.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Document your application allow list. 2. Implement technical controls enforcing the allow list. 3. Establish a process for requesting and approving new software. 4. Review and update the allow list regularly.	Windows Defender Application Control (WDAC) policy. AppLocker rules. Third-party endpoint protection with application control.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ Application allow list documentation.
■ Technical control configuration for application execution.
■ Software request and approval process.
■ Regular allow list review records.

■ Assessor Notes

Deny-by-default posture is a significant security improvement over traditional approaches.

Your Notes:

CM.L2-3.4.9 Configuration Management User-Installed Software

SPRS Weight –3

Official Requirement (NIST SP 800-171 Rev 2):

"Control and monitor user-installed software."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Prevent users from installing software without authorization. User-installed software is a major source of malware.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Remove local administrator rights from standard users. 2. Require IT approval for any software installation. 3. Monitor for unauthorized software installations. 4. Implement software asset management.	Windows Group Policy: restrict software installation to admins only. Microsoft Intune software catalog. Software asset management tools. Regular software inventory audits.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Evidence that standard users cannot install software.
- Software approval process documentation.
- Recent software inventory audit.
- Monitoring configuration for unauthorized software.

Assessor Notes

Removing local admin rights simultaneously satisfies portions of AC least privilege controls and this CM control.

Your Notes:

I
A

Identification & Authentication

11 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
IA.L2-3.5.1	User Identification	**–3 pts**	Met Partial Not Met
IA.L2-3.5.2	User Authentication	**–3 pts**	Met Partial Not Met
IA.L2-3.5.3	Multi-Factor Authentication	**–5 pts**	Met Partial Not Met
IA.L2-3.5.4	Replay-Resistant Authentication	**–3 pts**	Met Partial Not Met
IA.L2-3.5.5	Identifier Reuse	**–1 pts**	Met Partial Not Met
IA.L2-3.5.6	Identifier Handling	**–1 pts**	Met Partial Not Met
IA.L2-3.5.7	Password Complexity	**–3 pts**	Met Partial Not Met
IA.L2-3.5.8	Password Reuse	**–1 pts**	Met Partial Not Met
IA.L2-3.5.9	Temporary Passwords	**–1 pts**	Met Partial Not Met

IA.L2-3.5.10	Cryptographic Password Protection	**–3 pts**	Met Partial Not Met
IA.L2-3.5.11	Obscure Feedback	**–1 pts**	Met Partial Not Met

IA.L2-3.5.1 Identification & Authentication

User Identification

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Every person, automated process, and device that accesses your systems must have a unique identity. No anonymous access, no shared 'guest' accounts used for real work. NOTE: This requirement is also a CMMC Level 1 control covered in WB2.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Assign a unique username to every person who accesses any system. 2. Remove or disable generic accounts (admin, user, guest). 3. Ensure automated processes have their own named identities. 4. Document all system identities in your asset and user inventory.	Windows local accounts or Active Directory. Microsoft 365 named user licenses. Disable built-in Guest account on all computers.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Full list of user accounts showing each has a unique identifier.
- ■ Evidence that guest/anonymous accounts are disabled.
- ■ Asset inventory showing devices are identified.

■ Assessor Notes

Also covered as a Level 1 requirement (IA.L1-3.5.1 in WB2). At Level 2, ensure documentation and evidence meet the higher assessment standard.

Your Notes:

IA.L2-3.5.2

Identification & Authentication
User Authentication

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

After identifying who someone is, you must verify it — typically with a password. Everyone must log in before accessing any CUI system. NOTE: This requirement is also a CMMC Level 1 control covered in WB2.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Require passwords on all computers, laptops, and mobile devices. 2. Set password complexity requirements. 3. Enable automatic screen lock after 15 minutes of inactivity. 4. Require passwords on all shared drives, cloud services, and email accounts.	Windows: Settings → Accounts → Sign-in options. Microsoft 365: password policies in Admin Center. MFA strongly recommended at Level 1 and required at Level 2 (see IA.L2-3.5.3).

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Password policy documentation showing complexity requirements.
- ■ Screenshots of system sign-in requirements.
- ■ Screen lock timeout settings on all devices.
- ■ Evidence that default/blank passwords have been changed.

■ Assessor Notes

Also covered as a Level 1 requirement (IA.L1-3.5.2 in WB2). At Level 2, document that this is implemented and pair with IA.L2-3.5.3 (MFA).

Your Notes:

IA.L2-3.5.3

Identification & Authentication
Multi-Factor Authentication

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Require MFA for all access to CUI systems — especially privileged accounts and all remote/network access. MFA is the single most effective control against account compromise.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Enable MFA for all Microsoft 365/Azure AD accounts. 2. Require MFA for all VPN and remote access. 3. Enforce MFA for all privileged account logons. 4. Use authenticator apps (not SMS) where possible. 5. Document MFA enforcement in SSP.	Microsoft Authenticator app. Azure AD MFA (included in M365 Business Premium). Duo Security. YubiKey hardware tokens. Enable via Conditional Access policies.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ MFA enrollment records for all users.
- ■ Conditional Access policy requiring MFA.
- ■ Evidence MFA cannot be bypassed.
- ■ MFA enforcement for privileged accounts.

■ Assessor Notes

MFA is the single highest-impact control in this entire list. Enable it immediately — prevents the vast majority of account compromise attacks.

Your Notes:

IA.L2-3.5.4 Identification & Authentication
Replay-Resistant Authentication

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ *enter here*

Assessor: ■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Use authentication mechanisms that cannot be defeated by capturing and replaying authentication data.

WHAT YOU NEED TO DO

1. Ensure VPN uses modern, replay-resistant authentication protocols.
2. Use Kerberos or TLS-based authentication (not legacy NTLM where possible).
3. Implement FIDO2 or certificate-based authentication for privileged accounts.
4. Disable or restrict legacy authentication protocols.

COMMON SMALL BUSINESS SOLUTIONS

Azure AD with modern authentication. Kerberos (Windows default for domain accounts). FIDO2 security keys. Disable legacy authentication in M365 Conditional Access.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Authentication protocol configuration showing replay-resistant mechanisms.
- ■ Evidence that legacy authentication is restricted.
- ■ Modern authentication configuration for Microsoft 365.

■ Assessor Notes

Disabling legacy authentication in Microsoft 365 is free, quick, and dramatically reduces attack surface.

Your Notes:

IA.L2-3.5.5

Identification & Authentication
Identifier Reuse

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Employ the following measures to manage identifiers: prohibit reuse of identifiers for a defined period."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Once a user account identifier is deactivated, do not reuse that same identifier for a new user for a defined period.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Establish a policy prohibiting reuse of account identifiers for at least 2 years. 2. Verify username is not a recently retired one when creating accounts. 3. Document identifier management policy.	Active Directory account naming convention that avoids reuse. Manual verification process when creating accounts.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Identifier reuse policy documentation.
- ■ Account creation procedure including reuse check.
- ■ Evidence of policy enforcement.

■ Assessor Notes

Identifier reuse can cause access control confusion if the old account had residual permissions.

Your Notes:

IA.L2-3.5.6	Identification & Authentication Identifier Handling	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Employ the following measures to manage identifiers: disable identifiers after a defined inactivity period."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Automatically disable accounts that have not been used within a defined period (e.g., 90 days). Dormant accounts are a security risk.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Configure automatic account disabling for accounts inactive more than 90 days. 2. Review inactive accounts at least quarterly. 3. Disable accounts for contractors and vendors immediately when engagement ends. 4. Document inactive account policy.	Active Directory: Account Expires setting. Azure AD: Stale accounts report. PowerShell scripts to identify and disable inactive accounts.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ Inactive account policy documentation.
■ Evidence of automatic or periodic inactive account disabling.
■ Recent inactive account audit records.

■ Assessor Notes

Contractor and vendor accounts left active after engagement ends are a chronic compliance gap.

Your Notes:

IA.L2-3.5.7

Identification & Authentication
Password Complexity

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Enforce a minimum password complexity and change requirements for passwords used on organizational systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Require passwords to be sufficiently complex to resist guessing and brute force attacks.

WHAT YOU NEED TO DO

1. Set minimum password length of 12+ characters.
2. Require mix of character types OR length-only policy with 15+ characters (per NIST SP 800-63B).
3. Enforce via Group Policy or identity provider.
4. Prohibit common and previously used passwords.

COMMON SMALL BUSINESS SOLUTIONS

Windows Group Policy: Fine-grained password policies. Azure AD Password Protection (blocks common passwords — free). NIST SP 800-63B recommends length over complexity.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Password policy configuration showing complexity requirements.
- ■ Azure AD Password Protection configuration.
- ■ Evidence policy is enforced on all systems.

■ Assessor Notes

NIST currently recommends focusing on LENGTH (15+ chars) over complexity rules — both satisfy this control.

Your Notes:

IA.L2-3.5.8 Identification & Authentication
Password Reuse

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Prohibit password reuse for a specified number of generations."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ *enter here*

Assessor: ■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Prevent users from cycling back to previously used passwords.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Configure password history to remember at least 24 previous passwords. 2. Enforce via Group Policy or identity provider. 3. Document password history policy. 4. Apply to all CUI systems.	Windows Group Policy: Enforce password history (set to 24). Azure AD password history (enforced automatically).

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Password history policy configuration showing 24+ generations.
- ■ Evidence of enforcement across all in-scope systems.
- ■ Password policy documentation.

■ Assessor Notes

Simple Group Policy setting — configure once and it enforces automatically.

Your Notes:

IA.L2-3.5.9

Identification & Authentication
Temporary Passwords

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Allow temporary passwords for system logons with an immediate change requirement."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ enter here

Assessor:
■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When issuing temporary passwords, require the user to change the password immediately upon first logon.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Configure all new accounts to require password change at first logon. 2. Set temporary passwords to expire within 24 hours if not used. 3. Apply to all password reset procedures. 4. Document temporary password policy.	Active Directory: User must change password at next logon. Azure AD: Temporary access passes.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ AD/Azure AD configuration showing immediate change requirement.
- ■ IT helpdesk password reset procedure documentation.
- ■ Evidence of policy enforcement.

■ Assessor Notes

Check 'User must change password at next logon' for all new and reset accounts — takes seconds to configure.

Your Notes:

IA.L2-3.5.10 Identification & Authentication
Cryptographic Password Protection

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Store and transmit only cryptographically-protected passwords."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ enter here

Assessor: ■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Passwords must never be stored in plaintext or transmitted unencrypted. Use strong hashing for storage and encrypted channels for transmission.

WHAT YOU NEED TO DO

1. Verify all authentication systems use strong password hashing (bcrypt, PBKDF2, Argon2, or SHA-256 minimum).
2. Ensure all password transmission occurs over encrypted channels (TLS 1.2+).
3. Disable legacy protocols that transmit credentials in cleartext.
4. Audit any internally developed applications for plaintext password storage.

COMMON SMALL BUSINESS SOLUTIONS

Active Directory uses Kerberos and NTLM hashing. Modern identity providers use strong hashing. TLS for all web applications.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Documentation of password hashing mechanisms used.
- ■ Evidence that plaintext password protocols are disabled.
- ■ TLS configuration for all authentication interfaces.

■ Assessor Notes

This primarily applies to custom applications. Commercial systems (Windows AD, M365) handle this correctly by default — document that.

Your Notes:

IA.L2-3.5.11 Identification & Authentication
Obscure Feedback

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Obscure feedback of authentication information."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When users enter passwords, they must not be displayed on screen. Password fields must show asterisks or dots.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Verify all login interfaces obscure password entry. 2. Audit any custom applications for authentication feedback obscuring. 3. Verify web-based admin interfaces obscure passwords. 4. Document any exceptions with risk justification.	Standard browser and OS behavior for password fields. Verify custom-developed applications. Most commercial software does this by default.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Evidence of testing login interfaces for password obscuring.
- Documentation of any custom application review.
- Screenshots confirming password fields are obscured.

Assessor Notes

For standard commercial software this is already implemented. Key is auditing any custom or legacy applications.

Your Notes:

I
R

Incident Response

3 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
IR.L2-3.6.1	Incident Handling	**–5 pts**	Met Partial Not Met
IR.L2-3.6.2	Incident Reporting	**–5 pts**	Met Partial Not Met
IR.L2-3.6.3	Incident Response Testing	**–3 pts**	Met Partial Not Met

IR.L2-3.6.1

Incident Response
Incident Handling

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Have a formal, documented incident response (IR) plan and capability covering all phases of incident handling.

WHAT YOU NEED TO DO

1. Develop a written Incident Response Plan (IRP) covering preparation, detection, analysis, containment, eradication, and recovery.
2. Define roles and responsibilities for incident response.
3. Establish communication procedures including DoD reporting.
4. Test the IRP annually through tabletop exercises.
5. Document in SSP.

COMMON SMALL BUSINESS SOLUTIONS

NIST SP 800-61 incident response framework. CISA incident response resources. SANS sample IR plans. Microsoft 365 Defender for detection.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Written Incident Response Plan.
- Role and responsibility assignments.
- Communication plan including DoD reporting requirements.
- Annual tabletop exercise records.

Assessor Notes

DFARS 252.204-7012 requires reporting cyber incidents to DoD within 72 hours. Your IRP must include this requirement.

Your Notes:

IR.L2-3.6.2

Incident Response
Incident Reporting

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When incidents occur, track and document them and report to appropriate external parties including the DoD.

WHAT YOU NEED TO DO

1. Establish an incident tracking system.
2. Define internal escalation and reporting procedures.
3. Implement DoD reporting per DFARS 252.204-7012 (report within 72 hours to dibnet.dod.mil).
4. Define what constitutes a reportable incident.

COMMON SMALL BUSINESS SOLUTIONS

DIBNet portal (dibnet.dod.mil) for DoD reporting. Internal ticketing system. CISA reporting for significant incidents.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Incident tracking log or system.
- ■ Internal reporting procedure documentation.
- ■ DoD incident reporting procedure (DFARS compliance).
- ■ Records of any incidents reported.

■ Assessor Notes

The 72-hour DoD reporting requirement is mandatory regardless of CMMC level. Ensure your team knows this.

Your Notes:

IR.L2-3.6.3

Incident Response
Incident Response Testing

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Test the organizational incident response capability."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Regularly test your incident response capabilities through exercises, simulations, or drills.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Conduct annual tabletop exercises simulating realistic incident scenarios. 2. Test technical IR capabilities (detection, containment, recovery). 3. Include external reporting procedures in exercises. 4. Document exercise results and update IRP based on findings.	CISA tabletop exercise templates (free). SANS incident response exercise frameworks.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Annual tabletop exercise documentation.
- ■ IR plan updates from exercise findings.
- ■ Technical capability test records.

■ Assessor Notes

Even a 2-hour tabletop exercise dramatically improves IR readiness. Use CISA's free exercise templates.

Your Notes:

MA Maintenance

6 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
MA.L2-3.7.1	Managed Maintenance	**–3 pts**	Met Partial Not Met
MA.L2-3.7.2	Controlled Maintenance	**–3 pts**	Met Partial Not Met
MA.L2-3.7.3	Equipment Sanitization	**–3 pts**	Met Partial Not Met
MA.L2-3.7.4	Media Inspection	**–3 pts**	Met Partial Not Met
MA.L2-3.7.5	Nonlocal Maintenance	**–3 pts**	Met Partial Not Met
MA.L2-3.7.6	Maintenance Personnel	**–3 pts**	Met Partial Not Met

MA.L2-3.7.1

Maintenance
Managed Maintenance

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Perform maintenance on organizational systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

System maintenance must be performed in a controlled, documented manner that does not create security vulnerabilities.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Document all system maintenance activities (what, when, by whom). 2. Require approval for significant maintenance activities. 3. Verify system integrity and security after maintenance. 4. Include maintenance procedures in SSP.	IT service management system. Maintenance log spreadsheet. Scheduled maintenance windows. Post-maintenance security verification checklist.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Maintenance log showing all activities.
- Maintenance authorization records.
- Post-maintenance verification records.
- Maintenance policy in SSP.

Assessor Notes

Maintenance covers both hardware and software. Include OS patches, hardware repairs, and vendor visits in your maintenance log.

Your Notes:

MA.L2-3.7.2 Maintenance
Controlled Maintenance

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Control the tools and people used for maintenance. Remote maintenance must be particularly controlled.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Approve and inventory all maintenance tools used on CUI systems. 2. Control and monitor remote maintenance sessions. 3. Require MFA for remote maintenance access. 4. Terminate remote sessions immediately after work is complete.	Approved maintenance tool list. Remote support tools with session logging (TeamViewer, ConnectWise). Monitor and record remote sessions.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Approved maintenance tools list.
- ■ Remote maintenance session logs.
- ■ MFA requirement for remote maintenance.
- ■ Procedure for terminating remote sessions.

■ Assessor Notes

Vendor support sessions are a common attack vector. Always monitor remote support sessions and terminate immediately when complete.

Your Notes:

MA.L2-3.7.3

Maintenance
Equipment Sanitization

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Before sending equipment for off-site repair, remove or sanitize all CUI from the device.

WHAT YOU NEED TO DO

1. Establish a procedure for sanitizing equipment before off-site maintenance.
2. Use approved sanitization methods (wipe, encryption, or media removal).
3. Document all equipment sent off-site and sanitization performed.
4. Verify sanitization is complete before release.

COMMON SMALL BUSINESS SOLUTIONS

BitLocker key deletion effectively wipes encrypted drives. DBAN for full wiping before repair. Document sanitization in maintenance log.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Equipment sanitization procedure documentation.
- ■ Records of equipment sent off-site with sanitization method.
- ■ Sanitization verification records.

■ Assessor Notes

A BitLocker-encrypted drive with its key deleted is effectively wiped — faster than a full wipe for off-site maintenance.

Your Notes:

MA.L2-3.7.4 Maintenance Media Inspection

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Before connecting any external media used for maintenance to your systems, scan it for malware.

WHAT YOU NEED TO DO

1. Require antivirus scanning of all maintenance media before use.
2. Use organization-provided, pre-scanned media for diagnostics where possible.
3. Do not connect vendor-provided USB drives without prior scanning.
4. Document media inspection requirement in maintenance policy.

COMMON SMALL BUSINESS SOLUTIONS

Scan maintenance USB drives with updated antivirus before connecting. Dedicated scanning workstation for vendor media.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Maintenance media scanning policy.
- ■ Antivirus scan records for maintenance media.
- ■ Evidence that scanning occurs before connection.

■ Assessor Notes

Vendor-provided USB drives have been used as malware delivery vectors. Scan everything before connecting to CUI systems.

Your Notes:

MA.L2-3.7.5

Maintenance
Nonlocal Maintenance

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Require MFA for all non-local maintenance sessions and ensure maintenance is monitored."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Remote maintenance sessions must use multi-factor authentication and be monitored by an authorized local administrator.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Require MFA for all remote/non-local maintenance sessions. 2. Monitor all remote maintenance sessions (local administrator present or watching). 3. Log all non-local maintenance session details. 4. Disconnect idle non-local maintenance sessions.	Remote support tools with MFA (TeamViewer with 2FA, ConnectWise with MFA). Session recording. Policy requiring local monitor for remote maintenance.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ MFA configuration for remote maintenance access.
- ■ Session monitoring records or recordings.
- ■ Remote maintenance session logs.
- ■ Local monitor requirement in maintenance policy.

Assessor Notes

Never leave remote vendor access unattended. An employee watching the session is a simple but effective control.

Your Notes:

MA.L2-3.7.6

Maintenance
Maintenance Personnel

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When maintenance is performed by personnel who lack CUI access authorization, they must be supervised.

WHAT YOU NEED TO DO

1. Identify maintenance personnel who lack required CUI access authorization.
2. Require supervision of all such personnel during maintenance.
3. Restrict unsupervised maintenance personnel from accessing CUI.
4. Document supervision requirements in maintenance policy.

COMMON SMALL BUSINESS SOLUTIONS

Escort and supervision policy. Visitor escort procedures. Clean-desk procedures to hide CUI during maintenance.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ List of authorized vs. unauthorized maintenance personnel.
- ■ Supervision policy and records.
- ■ Evidence that CUI is protected during maintenance activities.

■ Assessor Notes

This applies to HVAC technicians, electricians, copier repair persons — anyone doing maintenance in spaces with CUI systems.

Your Notes:

MP Media Protection

9 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
MP.L2-3.8.1	Media Protection	**–3 pts**	Met Partial Not Met
MP.L2-3.8.2	Media Access	**–3 pts**	Met Partial Not Met
MP.L2-3.8.3	Media Sanitization	**–3 pts**	Met Partial Not Met
MP.L2-3.8.4	Media Markings	**–3 pts**	Met Partial Not Met
MP.L2-3.8.5	Media Accountability	**–3 pts**	Met Partial Not Met
MP.L2-3.8.6	Portable Storage Encryption	**–5 pts**	Met Partial Not Met
MP.L2-3.8.7	Removable Media	**–3 pts**	Met Partial Not Met
MP.L2-3.8.8	Shared Media	**–1 pts**	Met Partial Not Met
MP.L2-3.8.9	Protect Backups	**–5 pts**	Met Partial Not Met

MP.L2-3.8.1

Media Protection
Media Protection

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Physically protect all media containing CUI — hard drives, USB drives, printed documents, and any other medium storing CUI.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Identify all media containing CUI (digital and paper). 2. Store CUI media in locked storage when not in use. 3. Implement a media handling policy. 4. Label CUI media appropriately. 5. Track CUI media inventory.	Locked cabinets or safes for paper CUI. Encrypted storage for digital media. Media inventory system. CUI cover sheets for paper documents.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ CUI media inventory.
- ■ Physical storage protection evidence.
- ■ Media handling policy.
- ■ CUI labeling evidence.

■ Assessor Notes

Paper CUI is often overlooked. Ensure printed CUI is stored securely and not left on desks.

Your Notes:

MP.L2-3.8.2

Media Protection
Media Access

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

"Limit access to CUI on system media to authorized users."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Only authorized users should be able to access media containing CUI.

WHAT YOU NEED TO DO

1. Implement access controls on all CUI storage systems.
2. Restrict physical access to storage areas with CUI media.
3. Maintain a list of personnel authorized to access CUI media.
4. Audit access to CUI media regularly.

COMMON SMALL BUSINESS SOLUTIONS

File and folder permissions on digital media. Physical access controls on storage rooms. CUI media access log. Encryption.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Access control configuration for digital CUI storage.
- ■ Physical access restrictions for CUI media storage.
- ■ CUI media access authorization list.

■ Assessor Notes

If access controls on your systems are properly implemented, media access is largely addressed through AC controls.

Your Notes:

MP.L2-3.8.3

Media Protection
Media Sanitization

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Sanitize or destroy system media before disposal or reuse."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

All media must be sanitized before disposal or reuse, following NIST SP 800-88 compliant procedures.

WHAT YOU NEED TO DO

1. Use NIST SP 800-88 compliant sanitization methods.
2. Maintain a complete media sanitization log.
3. Obtain certificates of destruction for third-party sanitization.
4. Apply to ALL media types (drives, USB, phones, paper shredding).

COMMON SMALL BUSINESS SOLUTIONS

DBAN for HDDs. Manufacturer secure erase for SSDs. NSA/CSS EPL-listed degaussers. Paper shredders (cross-cut minimum). NIST SP 800-88 guidance.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Media sanitization log with all disposals documented.
- ■ NIST SP 800-88 compliant sanitization procedures.
- ■ Certificates of destruction for third-party sanitization.
- ■ Paper shredding policy and equipment documentation.

■ Assessor Notes

At Level 2, document your sanitization procedures explicitly and reference NIST SP 800-88.

Your Notes:

MP.L2-3.8.4

Media Protection
Media Markings

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Mark media with necessary CUI markings and distribution limitations."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

All media containing CUI must be labeled with appropriate CUI markings.

WHAT YOU NEED TO DO

1. Label all removable media containing CUI with CUI markings.
2. Apply CUI cover sheets to printed documents.
3. Train employees on CUI marking requirements.
4. Implement a marking policy per National Archives CUI Registry requirements.

COMMON SMALL BUSINESS SOLUTIONS

CUI labels from National Archives (archives.gov/cui). Label printers. Digital metadata tagging. Microsoft Purview sensitivity labels.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ CUI marking policy referencing National Archives requirements.
- ■ Sample labeled media and documents.
- ■ Training records on CUI marking.
- ■ Sensitivity label configuration if using Microsoft Purview.

■ Assessor Notes

The National Archives CUI Registry (archives.gov/cui) defines exact marking requirements. Use their official language.

Your Notes:

MP.L2-3.8.5

Media Protection
Media Accountability

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Control access to media containing CUI and maintain accountability for media during transport."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Track and account for all media containing CUI, especially during transport.

WHAT YOU NEED TO DO

1. Maintain a media inventory tracking all CUI media.
2. Log all media check-out and check-in events.
3. Require encryption for CUI media transported outside your facility.
4. Use chain-of-custody procedures for media transport.

COMMON SMALL BUSINESS SOLUTIONS

Media inventory spreadsheet. Check-out/in log. BitLocker encrypted USB drives. Courier services with chain-of-custody tracking.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Media inventory showing all CUI media.
- ■ Media transport log with chain-of-custody records.
- ■ Encryption evidence for transported media.
- ■ Media transport policy.

■ Assessor Notes

USB drives containing CUI must be encrypted before leaving your facility. BitLocker To Go is free and effective.

Your Notes:

MP.L2-3.8.6

Media Protection
Portable Storage Encryption

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

"Implement cryptographic mechanisms to protect the confidentiality of CUI during transport unless otherwise protected by alternative physical safeguards."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Encrypt CUI when transported on portable media. Physical transport of unencrypted CUI media is prohibited.

WHAT YOU NEED TO DO

1. Enable BitLocker To Go on all USB drives used to transport CUI.
2. Encrypt all laptops with BitLocker or FileVault.
3. Use encrypted email or secure file transfer for electronic CUI transmission.
4. Verify encryption before transporting any CUI media.

COMMON SMALL BUSINESS SOLUTIONS

BitLocker To Go (Windows — free, built-in). VeraCrypt (free, cross-platform). M365 Message Encryption. SFTP, FTPS, or HTTPS for file transfer.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ USB drive encryption configuration.
- ■ Laptop full-disk encryption status.
- ■ Secure transmission method documentation.
- ■ Policy requiring encryption for CUI transport.

■ Assessor Notes

BitLocker To Go takes minutes to enable on a USB drive and is free. No excuse for unencrypted CUI transport.

Your Notes:

MP.L2-3.8.7 Media Protection Removable Media

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Control the use of removable media on system components."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Manage and control the use of removable media (USB drives, external drives, CDs) on CUI systems.

WHAT YOU NEED TO DO

1. Implement policy controlling removable media use.
2. Restrict removable media to authorized, encrypted devices only.
3. Log removable media connection events.
4. Prohibit personal USB drives on CUI systems.

COMMON SMALL BUSINESS SOLUTIONS

Group Policy: Removable Storage Access restrictions. Device control solutions. Audit policy for removable media insertion.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Removable media policy.
- ■ Group Policy configuration restricting removable media.
- ■ Audit logs showing removable media events.
- ■ Approved media list.

■ Assessor Notes

Ties to AC.L2-3.1.21. Implement both policy restriction and technical enforcement via Group Policy.

Your Notes:

MP.L2-3.8.8

Media Protection
Shared Media

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Prohibit the use of portable storage devices when such devices have no identifiable owner."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Do not connect unidentified or 'found' USB drives to your systems.

WHAT YOU NEED TO DO

1. Establish a policy prohibiting unidentified storage devices.
2. Train employees never to plug in found USB drives.
3. Include 'found USB drive' scenario in security awareness training.
4. Implement technical controls to block unrecognized devices.

COMMON SMALL BUSINESS SOLUTIONS

Device whitelisting via Group Policy. Security awareness training content on USB baiting attacks. Device control requiring device registration.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Policy prohibiting unidentified storage devices.
- ■ Training records showing employees trained on this risk.
- ■ Technical controls preventing unregistered device connection.

■ Assessor Notes

USB baiting is a real and effective attack technique. Train employees — it takes 10 minutes in security awareness training.

Your Notes:

MP.L2-3.8.9 Media Protection Protect Backups

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

"Protect the confidentiality of backup CUI at storage locations."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ enter here

Assessor:
■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Backup copies of CUI must be protected with the same rigor as primary copies.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Encrypt all backup media containing CUI. 2. Restrict access to backup systems and media. 3. Store backup copies in a secure, separate location. 4. Test backup restoration regularly. 5. Document backup protection in SSP.	Encrypted cloud backup (Azure Backup, Veeam with encryption). BitLocker on backup drives. Off-site or cloud storage with access controls.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Backup encryption configuration.
- ■ Access control configuration for backup systems.
- ■ Off-site or separate storage evidence.
- ■ Backup restoration test records.

■ Assessor Notes

Unencrypted backups stored alongside primary data defeat the purpose of backups for security.

Your Notes:

PE Physical Protection

6 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
PE.L2-3.10.1	Limit Physical Access	**–3 pts**	Met Partial Not Met
PE.L2-3.10.2	Monitor Physical Access	**–3 pts**	Met Partial Not Met
PE.L2-3.10.3	Visitor Control	**–3 pts**	Met Partial Not Met
PE.L2-3.10.4	Physical Access Logs	**–3 pts**	Met Partial Not Met
PE.L2-3.10.5	Manage Physical Access Devices	**–3 pts**	Met Partial Not Met
PE.L2-3.10.6	Alternative Work Sites	**–3 pts**	Met Partial Not Met

PE.L2-3.10.1 Physical Protection
Limit Physical Access

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Limit physical access to organizational systems to authorized individuals."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Formal physical access control for CUI systems with additional documentation requirements beyond Level 1.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Implement formal physical access control system (keycards, PIN pads). 2. Maintain a current list of all personnel with physical access authorization. 3. Review and update physical access authorization at least annually. 4. Immediately revoke physical access upon employee departure. 5. Document in SSP.	Keycard access systems. PIN pad door locks. Electronic access control with audit logs.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Physical access authorization list with last review date.
- Physical access control system evidence.
- Annual access review records.
- Evidence of immediate access revocation upon departure.

Assessor Notes

Electronic access control systems generate audit logs needed for PE.L2-3.10.4. Consider upgrading from key locks.

Your Notes:

PE.L2-3.10.2

Physical Protection
Monitor Physical Access

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Monitor your facilities for unauthorized physical access through security cameras, alarms, or physical guards.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Install security cameras at entry/exit points and CUI system areas. 2. Implement intrusion detection (alarm system) for CUI facilities. 3. Monitor physical security alerts and investigate anomalies. 4. Retain camera footage for at least 90 days.	Security camera systems. Alarm systems. Physical security monitoring services.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Security camera installation evidence.
- ■ Alarm system configuration.
- ■ Camera footage retention policy.
- ■ Monitoring procedure documentation.

■ Assessor Notes

Basic security cameras and a business alarm system are affordable and satisfy this control.

Your Notes:

PE.L2-3.10.3 Physical Protection Visitor Control

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Escort visitors and monitor visitor activity."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Same as Level 1 with additional SSP documentation requirements at Level 2.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Maintain visitor log (name, org, date, time in/out, host). 2. Escort all visitors in CUI areas. 3. Brief employees on escorting requirements. 4. Review visitor logs regularly. 5. Document visitor control policy in SSP.	Visitor management software. Paper visitor log. Visitor badges. Document in SSP.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Visitor log records.
- Visitor control policy in SSP.
- Employee awareness records.
- Escort requirement enforcement evidence.

Assessor Notes

Keep logs for at least 90 days. The WB3 visitor log tab satisfies the logging requirement.

Your Notes:

PE.L2-3.10.4 Physical Protection
Physical Access Logs

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Maintain audit logs of physical access."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ *enter here*

Assessor: ■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Maintain and review records of physical access to facilities containing CUI systems.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Log all physical access events. 2. Retain logs for at least 90 days. 3. Review logs periodically for anomalies. 4. Protect logs from unauthorized modification.	Electronic access control logs. Visitor sign-in/out records. Security camera footage.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Physical access log records.
- ■ Log retention configuration/policy.
- ■ Evidence of periodic log review.

■ Assessor Notes

Electronic access control systems generate these logs automatically.

Your Notes:

PE.L2-3.10.5

Physical Protection
Manage Physical Access Devices

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Control and manage physical access devices."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Maintain inventory and control of all keys, keycards, and physical access devices.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Maintain an inventory of all physical access devices. 2. Record issuance of all access devices. 3. Immediately recover or deactivate access devices upon employee departure. 4. Conduct periodic inventory of physical access devices.	Access control management software. Key log spreadsheet. Keycard deactivation procedure. Access code change process.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Physical access device inventory.
- ■ Access device issuance log.
- ■ Deactivation/recovery records for departed employees.
- ■ Periodic inventory records.

■ Assessor Notes

For electronic access systems, deactivating a keycard is instant and logged. For physical keys, maintain a sign-out log and rekey when needed.

Your Notes:

PE.L2-3.10.6 Physical Protection
Alternative Work Sites

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Enforce safeguarding measures for CUI at alternative work sites."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When employees work from home or other locations outside the main office, CUI must be protected with equivalent safeguards.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Establish a remote work security policy covering CUI handling. 2. Require VPN for all remote work involving CUI. 3. Prohibit CUI on personal, unmanaged devices (unless MDM enrolled). 4. Train remote workers on physical security of CUI.	Remote work security policy. VPN requirement. MDM for remote devices. Physical security checklist for home offices.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Remote work security policy documentation.
- VPN usage evidence for remote work.
- Remote worker training records.
- Physical security requirements for home offices.

Assessor Notes

With remote work widespread, this control is increasingly important. A written remote work policy with physical security requirements satisfies this.

Your Notes:

P
S

Personnel Security

2 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
PS.L2-3.9.1	Screen Individuals	**–3 pts**	Met Partial Not Met
PS.L2-3.9.2	Protect CUI During Personnel Actions	**–5 pts**	Met Partial Not Met

PS.L2-3.9.1 Personnel Security
Screen Individuals

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Screen individuals prior to authorizing access to organizational systems containing CUI."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Conduct background screening of personnel before granting access to CUI systems.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Conduct background checks on all employees and contractors with CUI access. 2. Define screening requirements (criminal background check minimum). 3. Document screening results and access authorization decisions. 4. Include screening requirements in contractor agreements.	Background check vendors (Checkr, Sterling, HireRight). Reference DoD Personnel Security Program. Document in HR records.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Background check records for all CUI-access personnel.
- ■ Screening policy documentation.
- ■ Contractor agreement language requiring screening.
- ■ Documentation of screening-to-access authorization process.

■ Assessor Notes

At minimum, a basic criminal background check for all CUI-access personnel satisfies this control.

Your Notes:

PS.L2-3.9.2	Personnel Security Protect CUI During Personnel Actions	SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Have a formal process for protecting CUI when employees are terminated, transferred, or change roles.

WHAT YOU NEED TO DO

1. Create a formal offboarding checklist covering all access revocation steps.
2. Immediately revoke all system access upon termination.
3. Recover all CUI media, devices, and credentials from departing employees.
4. Transfer CUI responsibilities appropriately upon role changes.

COMMON SMALL BUSINESS SOLUTIONS

Offboarding checklist covering: AD account disable, M365 revocation, VPN access revoke, physical access deactivation, device recovery, credential rotation.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Offboarding checklist template.
- ■ Completed offboarding checklists for recent departures.
- ■ Evidence of immediate access revocation upon termination.
- ■ Device and media recovery records.

■ Assessor Notes

The offboarding process is a critical security control. A single missed step (active VPN for a terminated employee) can be catastrophic.

Your Notes:

RA

Risk Assessment

3 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
RA.L2-3.11.1	Risk Assessments	**–3 pts**	Met Partial Not Met
RA.L2-3.11.2	Vulnerability Scan	**–3 pts**	Met Partial Not Met
RA.L2-3.11.3	Remediate Vulnerabilities	**–5 pts**	Met Partial Not Met

RA.L2-3.11.1

Risk Assessment
Risk Assessments

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Conduct formal risk assessments at least annually to identify, evaluate, and prioritize security risks.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Conduct a formal risk assessment at least annually. 2. Identify threats relevant to your organization and CUI. 3. Assess likelihood and impact of identified threats. 4. Document risk assessment findings. 5. Use results to prioritize POA&M; items.	NIST SP 800-30 risk assessment methodology. CISA risk assessment tools. Risk register spreadsheet.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Annual risk assessment report.
- ■ Risk register with likelihood/impact ratings.
- ■ Evidence of risk assessment informing POA&M; and security decisions.

■ Assessor Notes

NIST SP 800-30 provides a free, authoritative methodology. Even a simplified version in a spreadsheet satisfies this control.

Your Notes:

RA.L2-3.11.2 Risk Assessment Vulnerability Scan

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Run regular vulnerability scans on all CUI systems. Scan frequency should increase for internet-facing systems.

WHAT YOU NEED TO DO

1. Run vulnerability scans on all in-scope systems at least monthly.
2. Increase scan frequency for internet-facing systems.
3. Scan immediately when critical CVEs are publicly disclosed.
4. Document scan methodology, tools, and results.
5. Feed findings into remediation process and POA&M.;

COMMON SMALL BUSINESS SOLUTIONS

Tenable Nessus Essentials (free up to 16 IPs). Qualys VMDR. Microsoft Defender Vulnerability Management. OpenVAS (free).

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Monthly vulnerability scan results.
- Scan configuration showing all in-scope systems covered.
- Critical vulnerability response procedure.
- Scan findings feeding into POA&M.;

Assessor Notes

Monthly scanning is the minimum. Critical CVEs (CVSS 9.0+) should trigger immediate scanning regardless of schedule.

Your Notes:

RA.L2-3.11.3

Risk Assessment
Remediate Vulnerabilities

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

"Remediate vulnerabilities in accordance with risk assessments."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Fix vulnerabilities within defined timeframes prioritized by risk.

WHAT YOU NEED TO DO

1. Define remediation SLAs by severity (Critical ≤15 days, High ≤30 days, Medium ≤90 days).
2. Track remediation in your vulnerability management system or POA&M.;
3. Verify remediation through rescanning.
4. Document exceptions with risk acceptance justification.

COMMON SMALL BUSINESS SOLUTIONS

Patch management tools. POA&M; tracking. Rescan after remediation. Risk acceptance process for exceptions.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Vulnerability remediation policy with defined SLAs.
- ■ Remediation tracking records.
- ■ Rescan evidence confirming fixes.
- ■ Risk acceptance documentation for exceptions.

■ Assessor Notes

The remediation SLA is not defined in the control — you define it in your policy. Critical ≤15 days, High ≤30 days, Medium ≤90 days is common practice.

Your Notes:

SC

System & Comm. Protection

16 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
SC.L2-3.13.1	Boundary Protection	**–5 pts**	Met Partial Not Met
SC.L2-3.13.2	Security Architecture	**–3 pts**	Met Partial Not Met
SC.L2-3.13.3	Role Separation	**–3 pts**	Met Partial Not Met
SC.L2-3.13.4	Shared Resource Control	**–3 pts**	Met Partial Not Met
SC.L2-3.13.5	Network Segmentation	**–3 pts**	Met Partial Not Met
SC.L2-3.13.6	Network Communication by Exception	**–5 pts**	Met Partial Not Met
SC.L2-3.13.7	Split Tunneling	**–3 pts**	Met Partial Not Met
SC.L2-3.13.8	Data in Transit Encryption	**–5 pts**	Met Partial Not Met
SC.L2-3.13.9	Connections Termination	**–1 pts**	Met Partial Not Met

SC.L2-3.13.10	Key Management	**–3 pts**	Met Partial Not Met
SC.L2-3.13.11	FIPS-Validated Cryptography	**–5 pts**	Met Partial Not Met
SC.L2-3.13.12	Collaborative Computing	**–1 pts**	Met Partial Not Met
SC.L2-3.13.13	Mobile Code	**–1 pts**	Met Partial Not Met
SC.L2-3.13.14	VoIP	**–1 pts**	Met Partial Not Met
SC.L2-3.13.15	Communications Authenticity	**–3 pts**	Met Partial Not Met
SC.L2-3.13.16	Data at Rest Protection	**–5 pts**	Met Partial Not Met

SC.L2-3.13.1

System & Comm. Protection
Boundary Protection

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

"Monitor, control, and protect communications at the external boundaries of the system and at key internal boundaries within the system."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Implement network boundary protection (firewalls, IDS/IPS) at your perimeter and between segments containing CUI.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Deploy and configure next-generation firewall at network perimeter. 2. Implement internal network segmentation to isolate CUI systems. 3. Monitor traffic at network boundaries. 4. Block unauthorized traffic at all boundaries. 5. Document network architecture in SSP.	Next-generation firewall (Palo Alto, Fortinet, Cisco ASA). Azure Firewall. Network segmentation via VLANs. IDS/IPS monitoring.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ Firewall configuration documentation.
■ Network diagram showing boundary protection.
■ Internal segmentation configuration.
■ IDS/IPS deployment evidence.

■ Assessor Notes

VLAN segmentation isolating CUI systems from general office traffic is a critical architectural improvement satisfying multiple SC controls.

Your Notes:

SC.L2-3.13.2

System & Comm. Protection
Security Architecture

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Design your system architecture with security as a design principle. Apply defense in depth.

WHAT YOU NEED TO DO

1. Document your system security architecture.
2. Apply principles: defense in depth, least privilege, fail-secure, separation of domains.
3. Segment CUI systems from general-purpose systems.
4. Review architecture when significant changes are made.

COMMON SMALL BUSINESS SOLUTIONS

Network diagrams. Architecture reviews. Defense-in-depth design. CIS Controls for architectural guidance. Document in SSP.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ System architecture documentation.
- ■ Network diagram showing security design principles.
- ■ Defense-in-depth architecture evidence.
- ■ Architecture review records.

■ Assessor Notes

A documented network architecture diagram is the foundation. If you don't have one, creating it while completing this assessment is a valuable first step.

Your Notes:

SC.L2-3.13.3

System & Comm. Protection
Role Separation

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Separate user functionality from system management functionality."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Keep user-facing and admin-facing systems and interfaces separated. Users access applications through user interfaces, not admin functions.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Separate application user interfaces from administrative interfaces. 2. Restrict administrative interface access to authorized admins only. 3. Use different authentication for admin and user functions. 4. Document role separation in SSP.	Separate admin consoles from user portals. Dedicated management networks. Admin-only workstations for system management.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Evidence of separated user and admin interfaces.
- ■ Access control for admin interfaces.
- ■ Dedicated management network or workstation evidence.

■ Assessor Notes

At minimum, ensure admin panels and management interfaces are not accessible by regular users.

Your Notes:

SC.L2-3.13.4 System & Comm. Protection Shared Resource Control

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

"Prevent unauthorized and unintended information transfer via shared system resources."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When multiple users share system resources, ensure one user's data cannot leak to another through shared resources.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Ensure OS enforces memory isolation between processes. 2. Use virtualization with proper isolation for multi-tenant environments. 3. Configure shared storage to prevent cross-user data access. 4. For cloud: use dedicated instances for CUI where possible.	Modern OS memory isolation (Windows, Linux). Hypervisor isolation in virtualized environments. Cloud: dedicated instances vs. shared. Encryption at rest.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- OS configuration showing memory/process isolation.
- Virtualization isolation configuration.
- Cloud service configuration showing appropriate isolation.

Assessor Notes

Modern operating systems handle this correctly by default. Cloud deployments need explicit review of isolation configurations.

Your Notes:

SC.L2-3.13.5	System & Comm. Protection Network Segmentation	SPRS Weight –3

Official Requirement (NIST SP 800-171 Rev 2):

"Implement subnetworks for publicly accessible system components that are separated from internal networks."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Public-facing systems must be in a DMZ or otherwise separated from internal CUI networks.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Implement a DMZ for any public-facing systems. 2. Ensure no direct routing between public and internal CUI systems. 3. Use firewall rules to control traffic between segments. 4. Document network segmentation in SSP.	VLAN-based segmentation. Physical network separation. DMZ firewalls. Cloud: separate VNets or subnets for public vs. private.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Network diagram showing DMZ and internal network separation.
- ■ Firewall rules between DMZ and internal networks.
- ■ Verification that no direct routing exists between public and internal systems.

■ Assessor Notes

If your company hosts any public-facing service, verify it is properly isolated from your internal CUI network.

Your Notes:

SC.L2-3.13.6

System & Comm. Protection
Network Communication by Exception

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Configure your network to block all traffic by default and only allow explicitly needed traffic.

WHAT YOU NEED TO DO

1. Configure all firewalls with default-deny rules.
2. Create explicit allow rules only for required traffic flows.
3. Review and document all allow rules with business justification.
4. Audit firewall rules regularly and remove unnecessary rules.

COMMON SMALL BUSINESS SOLUTIONS

Firewall default-deny configuration. Regular firewall rule review. Documented rules with justification. Network flow analysis.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Firewall configuration showing default-deny posture.
- ■ Documented firewall rules with business justification.
- ■ Regular firewall rule review records.
- ■ Evidence that unnecessary rules have been removed.

■ Assessor Notes

Many firewalls are deployed with overly permissive rules. A firewall rule review often reveals unnecessary access that should be removed.

Your Notes:

SC.L2-3.13.7 System & Comm. Protection Split Tunneling

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Prevent remote devices from simultaneously connecting with the system using VPN and other connections."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Disable VPN split tunneling so all remote device traffic flows through your VPN when connected.

WHAT YOU NEED TO DO

1. Disable split tunneling on all VPN configurations.
2. Test VPN to verify all traffic routes through the tunnel.
3. Document VPN configuration in SSP.
4. Monitor for split-tunnel configurations on managed devices.

COMMON SMALL BUSINESS SOLUTIONS

VPN client configuration: disable split tunneling. Test with IP leak check websites. Document in network security policy.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ VPN configuration showing split tunneling disabled.
- ■ Test results confirming all traffic routes through VPN.
- ■ VPN policy documentation.

■ Assessor Notes

Split tunneling allows remote devices to simultaneously access the internet directly (bypassing security controls) while connected to your network.

Your Notes:

SC.L2-3.13.8 System & Comm. Protection — Data in Transit Encryption

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Encrypt all CUI during network transmission — both internal and external.

WHAT YOU NEED TO DO

1. Use TLS 1.2 or higher for all web-based CUI transmission.
2. Use encrypted email for CUI email (TLS, S/MIME, or message encryption).
3. Use SFTP or FTPS for file transfer.
4. Disable weak encryption protocols (SSL, TLS 1.0, TLS 1.1).

COMMON SMALL BUSINESS SOLUTIONS

TLS 1.2/1.3 for web applications. Microsoft 365 Message Encryption. SFTP for file transfer. SSL Labs server test (free) to verify TLS configuration.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ TLS configuration on all web services (SSL Labs test results).
- ■ Email encryption configuration.
- ■ File transfer encryption evidence.
- ■ Evidence that weak protocols are disabled.

■ Assessor Notes

Use the free SSL Labs server test (ssllabs.com/ssltest) to verify TLS configuration. Aim for an A or A+ rating.

Your Notes:

SC.L2-3.13.9	System & Comm. Protection Connections Termination	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Terminate network connections associated with communications sessions after a defined period of inactivity."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Automatically terminate idle network sessions. This prevents attackers from hijacking abandoned sessions.

WHAT YOU NEED TO DO

1. Configure session timeouts for all network services (VPN, SSH, RDP, web apps).
2. Set VPN session timeout to no more than 4 hours of inactivity.
3. Configure web application session timeouts.
4. Document timeout values in network security policy.

COMMON SMALL BUSINESS SOLUTIONS

VPN session timeout settings. Web application session timeout configuration. SSH ClientAliveInterval settings. M365 session timeout policies.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ VPN timeout configuration.
- ■ Web application session timeout settings.
- ■ Network device session timeout configuration.
- ■ Documentation of defined timeout periods.

■ Assessor Notes

Idle session termination prevents session hijacking where an attacker takes over an unattended active session.

Your Notes:

SC.L2-3.13.10	System & Comm. Protection Key Management	SPRS Weight –3

Official Requirement (NIST SP 800-171 Rev 2):

"Establish and manage cryptographic keys for required cryptography employed in organizational systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Have a formal process for generating, storing, distributing, and destroying cryptographic keys.

WHAT YOU NEED TO DO

1. Document your cryptographic key management process.
2. Use key management systems or HSMs for critical keys.
3. Rotate encryption keys on a defined schedule.
4. Protect key material from unauthorized access.
5. Destroy keys when no longer needed.

COMMON SMALL BUSINESS SOLUTIONS

Windows Certificate Services. Azure Key Vault. BitLocker key management. PKI for certificate management.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Key management policy and procedures.
- ■ Key inventory (types, where used, rotation schedule).
- ■ Evidence of key rotation.
- ■ Key protection mechanisms.

Assessor Notes

At minimum, document what encryption keys you use, how they are stored, and your rotation schedule.

Your Notes:

SC.L2-3.13.11	System & Comm. Protection FIPS-Validated Cryptography	SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Use encryption algorithms validated under FIPS 140-2 or 140-3 to protect CUI.

WHAT YOU NEED TO DO

1. Enable FIPS mode on Windows systems via Group Policy.
2. Verify VPN uses FIPS-validated algorithms (AES-256, SHA-256, RSA-2048+).
3. Use FIPS-validated TLS for web applications.
4. Verify cloud services use FIPS-validated cryptography.
5. Document FIPS compliance in SSP.

COMMON SMALL BUSINESS SOLUTIONS

Windows FIPS mode (Group Policy: System cryptography → Use FIPS compliant algorithms). FIPS-validated VPN products. Azure services are FIPS-compliant. NIST CMVP database.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Windows FIPS mode configuration (GPO screenshot).
- ■ VPN product FIPS validation certificate.
- ■ Azure/cloud service FIPS compliance documentation.
- ■ SSP section on cryptographic standards.

■ Assessor Notes

Enable Windows FIPS mode via Group Policy. Most modern commercial products (M365, Azure VPN) use FIPS-validated algorithms — document this.

Your Notes:

SC.L2-3.13.12 System & Comm. Protection Collaborative Computing

SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ *enter here*

Assessor: ■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Collaborative devices (cameras, microphones) must not be remotely activated without user knowledge.

WHAT YOU NEED TO DO

1. Disable remote activation of cameras and microphones by default.
2. Ensure physical indicators (lights) show when devices are active.
3. Configure video conferencing tools to require user consent.
4. Train employees on collaborative computing security.

COMMON SMALL BUSINESS SOLUTIONS

Physical webcam covers. BIOS settings for camera/microphone disable. Windows privacy settings for app access. Policy on collaborative computing.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Policy on collaborative computing device use.
- ■ Evidence that remote activation is prevented or indicated.
- ■ Training records on collaborative computing security.

■ Assessor Notes

Physical webcam covers are a simple, cheap solution. Verify Windows privacy settings restrict app camera/microphone access.

Your Notes:

SC.L2-3.13.13	System & Comm. Protection Mobile Code	SPRS Weight −1

Official Requirement (NIST SP 800-171 Rev 2):

"Control and monitor the use of mobile code."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Control which mobile code (JavaScript, Java, ActiveX) is allowed to execute on your systems.

WHAT YOU NEED TO DO

1. Configure browsers to restrict or control mobile code execution.
2. Implement web content filtering to block malicious mobile code.
3. Disable ActiveX and Java in browsers where not needed.
4. Train users on risks of executing untrusted mobile code.

COMMON SMALL BUSINESS SOLUTIONS

Browser security settings. Web content filtering (Cisco Umbrella, Zscaler). Windows Defender SmartScreen. Disable Java and ActiveX.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Browser security configuration showing mobile code controls.
- ■ Web content filter configuration.
- ■ Evidence that unnecessary mobile code technologies are disabled.

■ Assessor Notes

Modern browsers have significantly reduced mobile code risks. Focus on keeping browsers updated and enabling SmartScreen.

Your Notes:

SC.L2-3.13.14	System & Comm. Protection VoIP	SPRS Weight –1

Official Requirement (NIST SP 800-171 Rev 2):

"Control and monitor the use of VoIP technologies."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

If your organization uses VoIP, ensure these communications are secured like other network communications.

WHAT YOU NEED TO DO

1. Inventory all VoIP systems and applications.
2. Ensure VoIP traffic is encrypted (SRTP for voice, TLS for signaling).
3. Segregate VoIP traffic on dedicated VLANs.
4. Monitor VoIP for abuse and unauthorized use.

COMMON SMALL BUSINESS SOLUTIONS

Encrypted VoIP (Teams, Zoom, Webex — all encrypt by default). VLAN segmentation. VoIP call monitoring where legally permissible.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ VoIP system inventory.
- ■ Encryption configuration for VoIP.
- ■ VLAN segregation for VoIP traffic.
- ■ VoIP monitoring and usage policy.

■ Assessor Notes

Microsoft Teams and Zoom encrypt voice/video by default. For traditional PBX systems, implement SRTP and TLS.

Your Notes:

SC.L2-3.13.15 System & Comm. Protection Communications Authenticity

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

"Protect the authenticity of communications sessions."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ *enter here*

Assessor: ■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Implement mechanisms to verify communications are authentic and have not been tampered with.

WHAT YOU NEED TO DO

1. Use TLS with valid certificates for all web communications.
2. Verify certificate validity in all client applications.
3. Implement email authentication (DKIM, DMARC, SPF) to prevent email spoofing.
4. Use authenticated protocols for inter-system communications.

COMMON SMALL BUSINESS SOLUTIONS

TLS certificates from trusted CAs. M365: DKIM and DMARC configuration. HSTS for web applications.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ TLS certificate configuration for all services.
- ■ DKIM, DMARC, and SPF configuration for email domain.
- ■ Certificate validation configuration in applications.

■ Assessor Notes

Configure DKIM, DMARC, and SPF for your email domain — free, quick, and significantly reduces email spoofing attacks.

Your Notes:

SC.L2-3.13.16	System & Comm. Protection Data at Rest Protection	SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

"Protect the confidentiality of CUI at rest."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Encrypt CUI when it is stored. This protects CUI if physical media is stolen or unauthorized access to storage occurs.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Enable full-disk encryption (BitLocker) on all computers and laptops. 2. Encrypt databases or file shares containing CUI. 3. Encrypt cloud storage containing CUI. 4. Verify encryption is enabled and functioning. 5. Document encryption configuration in SSP.	BitLocker (Windows — free, built-in). FileVault (Mac — free, built-in). Azure Storage encryption (automatic). SharePoint/OneDrive (included in M365). Database TDE.

EVIDENCE REQUIRED FOR GAP ASSESSMENT
■ BitLocker/FileVault status on all endpoints.
■ Database encryption configuration.
■ Cloud storage encryption configuration.
■ Encryption key management documentation.

■ Assessor Notes

BitLocker is free and built into Windows 10/11 Pro and Enterprise. Enable it on every laptop and desktop.

Your Notes:

SI System & Info. Integrity

7 Controls

Controls in this family:

Control ID	Control Name	SPRS Weight	Status
SI.L2-3.14.1	Flaw Remediation	**–5 pts**	Met Partial Not Met
SI.L2-3.14.2	Malicious Code Protection	**–3 pts**	Met Partial Not Met
SI.L2-3.14.3	Security Alerts, Advisories, and Directives	**–3 pts**	Met Partial Not Met
SI.L2-3.14.4	Update Malicious Code Protection	**–3 pts**	Met Partial Not Met
SI.L2-3.14.5	System and File Scanning	**–3 pts**	Met Partial Not Met
SI.L2-3.14.6	Security Monitoring	**–5 pts**	Met Partial Not Met
SI.L2-3.14.7	Identify Unauthorized Use	**–3 pts**	Met Partial Not Met

SI.L2-3.14.1 System & Info. Integrity Flaw Remediation

SPRS Weight –5

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Level 2 patch management requires a formal process with defined timelines and documentation.

WHAT YOU NEED TO DO

1. Implement a formal patch management process.
2. Run vulnerability scans monthly and after patch releases.
3. Patch Critical ≤15 days, High ≤30 days.
4. Track patching compliance and document exceptions.
5. Maintain patching records.

COMMON SMALL BUSINESS SOLUTIONS

WSUS for Windows patch management. Microsoft Endpoint Configuration Manager. Intune for cloud-based patch management. Vulnerability scanner integration.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Formal patch management policy with defined timelines.
- ■ Patch deployment records showing timely application.
- ■ Vulnerability scan results confirming patching.
- ■ POA&M; for delayed patches.

■ Assessor Notes

Automate patch deployment where possible. Windows WSUS is free. Manual patching at Level 2 scale is not sustainable.

Your Notes:

SI.L2-3.14.2	System & Info. Integrity Malicious Code Protection	SPRS Weight –3

Official Requirement (NIST SP 800-171 Rev 2):

"Provide protection from malicious code at appropriate locations within organizational systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Level 2 requires centralized endpoint protection management and reporting across all systems.

WHAT YOU NEED TO DO

1. Deploy endpoint protection on all systems with centralized management.
2. Implement centralized management and reporting.
3. Enable advanced threat protection features.
4. Configure real-time, behavioral, and signature-based detection.

COMMON SMALL BUSINESS SOLUTIONS

Microsoft Defender for Endpoint (included in M365 Business Premium). CrowdStrike Falcon Go. SentinelOne. Centralized management console required.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Centralized endpoint protection with all systems enrolled.
- ■ Management console showing all endpoints protected.
- ■ Real-time protection confirmation on all systems.
- ■ Advanced threat protection configuration.

■ Assessor Notes

Microsoft Defender for Endpoint (in M365 Business Premium) provides enterprise-grade protection with centralized management.

Your Notes:

SI.L2-3.14.3

System & Info. Integrity
Security Alerts, Advisories, and Directives

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

"Monitor system security alerts and advisories and take appropriate actions in response."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Stay current on security alerts and vulnerability disclosures affecting your systems and respond appropriately.

WHAT YOU NEED TO DO

1. Subscribe to security advisory feeds (Microsoft, CISA, NVD).
2. Establish a process for reviewing and acting on advisories.
3. Track advisory response activities.
4. Document advisory monitoring process.

COMMON SMALL BUSINESS SOLUTIONS

CISA Alerts (us-cert.cisa.gov/ncas). Microsoft Security Response Center (MSRC). NVD vulnerability feed. CISA Known Exploited Vulnerabilities catalog.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- Advisory monitoring subscription evidence.
- Process for reviewing and acting on advisories.
- Records of advisory response activities.

Assessor Notes

Subscribe to CISA's free email alerts (cisa.gov/subscribe-updates-cisa). MSRC provides monthly security update summaries for all Microsoft products.

Your Notes:

SI.L2-3.14.4

System & Info. Integrity
Update Malicious Code Protection

SPRS Weight —3

Official Requirement (NIST SP 800-171 Rev 2):

"Update malicious code protection mechanisms when new releases are available."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

At Level 2, verify and document that endpoint protection is current across all endpoints via centralized management.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Verify automatic definition updates are enabled and functioning on all endpoints. 2. Centrally monitor update status via management console. 3. Alert on endpoints with outdated definitions. 4. Document update verification process.	Microsoft Defender update management via Intune or MECM. Centralized endpoint protection console showing definition update status.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Centralized update status dashboard or report.
- ■ Alert configuration for stale definitions.
- ■ Policy requiring current definitions.
- ■ Update compliance report.

■ Assessor Notes

Your centralized endpoint protection console should show definition age for all enrolled devices. Alert on any device more than 24 hours behind.

Your Notes:

SI.L2-3.14.5

System & Info. Integrity
System and File Scanning

SPRS Weight −3

Official Requirement (NIST SP 800-171 Rev 2):

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

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ enter here

Assessor: ■ enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Level 2 requires centralized management, reporting, and documentation of scan activities across all endpoints.

WHAT YOU NEED TO DO

1. Configure real-time scanning on all endpoints.
2. Schedule regular full system scans (weekly minimum).
3. Use centralized management to verify scan compliance.
4. Review scan results and investigate detections.

COMMON SMALL BUSINESS SOLUTIONS

Microsoft Defender for Endpoint centralized scan management. Endpoint protection management console scan reports. Defender for Office 365 email scanning.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Centralized scan configuration showing all endpoints covered.
- ■ Scan completion reports from management console.
- ■ Real-time protection enabled on all endpoints.
- ■ Detection response records.

■ Assessor Notes

The difference from Level 1: centralized management providing visibility and reporting across all endpoints.

Your Notes:

SI.L2-3.14.6

System & Info. Integrity
Security Monitoring

SPRS Weight −5

Official Requirement (NIST SP 800-171 Rev 2):

"Monitor organizational systems, including the security of applications and services, to detect attacks and indicators of potential attacks."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Actively monitor your systems for signs of attacks. Go beyond log collection to actual threat detection.

WHAT YOU NEED TO DO

1. Implement security monitoring using SIEM or equivalent tools.
2. Configure detection rules for common attack patterns.
3. Monitor for indicators of compromise (IOCs).
4. Establish an alert response process.
5. Conduct periodic threat hunting.

COMMON SMALL BUSINESS SOLUTIONS

Microsoft Sentinel (SIEM). Microsoft Defender XDR (included in M365 Business Premium). Managed detection and response (MDR) services.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ SIEM or monitoring tool deployment evidence.
- ■ Detection rule configuration.
- ■ Alert response procedure.
- ■ Evidence of regular monitoring activities.

■ Assessor Notes

Microsoft Defender for Endpoint (in M365 Business Premium) provides significant security monitoring. Supplement with Microsoft Sentinel.

Your Notes:

SI.L2-3.14.7	System & Info. Integrity Identify Unauthorized Use	SPRS Weight –3

Official Requirement (NIST SP 800-171 Rev 2):

"Identify unauthorized use of organizational systems."

GAP ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
■ *enter here*

Assessor:
■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Be able to detect when your systems are being used in unauthorized ways by external attackers or internal users exceeding their authorized access.

WHAT YOU NEED TO DO

1. Define what constitutes authorized vs. unauthorized use.
2. Configure monitoring to detect and alert on unauthorized use.
3. Implement user and entity behavior analytics (UEBA) where feasible.
4. Investigate and document all detected unauthorized use incidents.

COMMON SMALL BUSINESS SOLUTIONS

Microsoft Sentinel UEBA. Microsoft Defender for Identity. Conditional Access anomaly detection. DLP alerts for unauthorized data access.

EVIDENCE REQUIRED FOR GAP ASSESSMENT

- ■ Definition of authorized use (acceptable use policy).
- ■ Monitoring configuration to detect unauthorized use.
- ■ Records of unauthorized use investigations.
- ■ UEBA tool deployment if applicable.

■ Assessor Notes

UEBA in Microsoft Sentinel can detect anomalous user behavior that traditional rule-based detection misses.

Your Notes:

NEXT STEPS AFTER COMPLETING THIS GAP ASSESSMENT

WB4 — System Security Plan (SSP) Starter

Develop or update your SSP to document how each of the 110 controls is implemented in your environment. The SSP is required for Level 2 assessment and must accurately describe your actual implementation — not planned implementation.

WB5 — POA&M; Tracker & SPRS Score Calculator

Enter all Not Met and Partially Met controls into WB5 as Plan of Action & Milestones (POA&M;) items. WB5 calculates your SPRS score automatically using the DoD assessment methodology. Submit your score to SPRS when ready.

WB6 — Pre-Assessment Readiness Checklist

Use WB6 as a final gate before submitting your self-assessment or engaging a C3PAO for third-party certification. WB6 covers documentation inventory, SPRS submission steps, affirmation requirements, and common assessment failure points.

This workbook is an educational and self-assessment tool. It does not constitute legal advice or a guarantee of CMMC compliance. Retain all completed assessment records for the duration of your contract plus three years. Re-evaluate any time your systems or contracts change.