# CMMC COMPLIANCE WORKBOOK SERIES

## WORKBOOK 6

# Pre-Assessment Readiness Checklist

Final Gate Before SPRS Submission or C3PAO Assessment

| | |
|---|---|
| **Use When:** | Before submitting your self-assessment to SPRS — or before engaging a C3PAO |
| **Works With:** | WB3 (Gap Assessment) + WB4 (SSP) + WB5 (POA&M;) → WB6 → SPRS submission |
| **Checklist Areas:** | 10 readiness domains covering documentation, evidence, people, and process |
| **Pass Threshold:** | All Critical items (★★★) must be checked before proceeding to assessment |
| **Version:** | 1.0 • March 2026 |

**■ USE THIS CHECKLIST SERIOUSLY**

A failed C3PAO assessment costs time, money, and may delay contract awards. A false self-assessment submitted to SPRS exposes your organization to False Claims Act liability. Work through every item in this checklist honestly before proceeding. If any Critical (★★★) item is unchecked, do not submit or schedule an assessment.

## HOW TO USE THIS CHECKLIST

This checklist is the final gate in the CMMC Workbook Series. It validates that all the work done in WB1 through WB5 has been completed correctly and that you are genuinely ready for either a self-assessment submission or a C3PAO third-party assessment.

| Priority | Label | Meaning | Action if Not Checked |
|---|---|---|---|
| ★★★ | **Critical** | Must be complete before proceeding. Non-negotiable. | Stop. Fix the gap before submitting or scheduling. |
| ★★☆ | **Important** | Strongly recommended. Gaps here increase assessment risk. | Fix before C3PAO. Document exception for self-assessment. |
| ★☆☆ | **Recommended** | Best practice. Not a blocker but improves confidence. | Note the gap and plan to address it post-assessment. |

### ■ Self-Assessment vs. C3PAO Assessment

This checklist applies to both. For a self-assessment (SPRS submission): all ★★★ items must be complete and the SSP must accurately describe your actual implementation. For a C3PAO third-party assessment: all ★★★ and ★★■ items should be complete. The C3PAO will compare your SSP statements to observed evidence — discrepancies are findings.

## DOMAIN 1 — Documentation Completeness

Assessors verify documentation before testing technical controls. Missing or outdated documents are immediate findings.

| DOCUMENTATION CHECKLIST | | |
|---|---|---|
| ■ | ★★★ **System Security Plan (SSP)** | SSP is complete, approved, and describes ACTUAL implementation (not aspirational). Version-controlled and dated within last 12 months. |
| ■ | ★★★ **All 110 Controls Addressed** | Every NIST SP 800-171 control has an implementation description in SSP Section 13. No blank or placeholder entries. |
| ■ | ★★★ **Network Diagram** | Current network diagram is attached to SSP Appendix A. Shows all in-scope assets, network segmentation, and external connections. |
| ■ | ★★★ **Asset Inventory** | Complete inventory of all hardware, software, and cloud services within the CUI boundary. Updated within last 90 days. |
| ■ | ★★★ **Authorized User List** | Current list of all users with CUI system access, their roles, and access levels. Reviewed within last 90 days. |
| ■ | ★★★ **POA&M; (if applicable)** | All gaps have a POA&M; entry in WB5 with specific corrective actions, responsible parties, and target dates within 180 days. |
| ■ | ★★☆ **Information Security Policy** | Written, approved, and communicated to all staff. References CUI handling requirements. |
| ■ | ★★☆ **Incident Response Plan** | Written IRP includes DoD 72-hour reporting requirement (DFARS 252.204-7012) and has been tested via tabletop exercise. |
| ■ | ★★☆ **All Supporting Policies** | Password policy, access control policy, remote work policy, media protection policy, patch management policy — all documented, approved, and current. |
| ■ | ★★☆ **External Connection Agreements** | ISA or equivalent agreement in place for every external system connection that can access CUI. |
| ■ | ★☆☆ **Change Log / Version History** | SSP shows version history with dates and descriptions of changes. At least one prior version documented. |
| ■ | ★☆☆ **Training Records** | Security awareness training completion records on file for all employees. Annual training completed. |

## DOMAIN 2 — Evidence Readiness

C3PAO assessors will request evidence for each control. Evidence must be organized, current, and directly tied to the controls it supports.

## EVIDENCE READINESS CHECKLIST

| | | |
|---|---|---|
| ■ | ★★★ **Evidence Folder Structure** | Evidence organized by control ID (e.g., /Evidence/AC.L2-3.1.1/). Assessors can quickly locate evidence for any control. |
| ■ | ★★★ **Screenshots are Current** | Configuration screenshots dated within 90 days. Outdated screenshots will not be accepted as evidence of current implementation. |
| ■ | ★★★ **MFA Evidence** | Screenshots showing MFA enrollment for ALL users. Conditional Access policy configuration. Evidence that MFA cannot be bypassed. |
| ■ | ★★★ **Encryption Evidence** | BitLocker status report showing all laptops/desktops encrypted. MDM compliance report for mobile devices. |
| ■ | ★★★ **Patch/Update Evidence** | Recent vulnerability scan results showing systems are patched. Patch management logs. No critical vulnerabilities unaddressed past SLA. |
| ■ | ★★★ **Audit Log Evidence** | Sample audit logs showing security events are being captured. Log retention configuration. Evidence logs are being reviewed. |
| ■ | ★★★ **Access Control Evidence** | User account list. Role-based permission configuration screenshots. Evidence of least privilege enforcement. |
| ■ | ★★☆ **Antivirus Evidence** | Centralized endpoint protection dashboard showing all systems enrolled and definitions current. |
| ■ | ★★☆ **Physical Security Evidence** | Visitor log records. Physical access log. Photos or description of physical access controls. |
| ■ | ★★☆ **Training Evidence** | Training completion certificates or records for all employees. Dated within last 12 months. |
| ■ | ★★☆ **Vendor/MSP Evidence** | ISA or contract clause for IT support. Evidence that remote vendor sessions are monitored and logged. |
| ■ | ★☆☆ **Penetration Test Report** | Annual penetration test report with findings and remediation status. Required for C3PAO — document rationale if not performed. |

## DOMAIN 3 — Technical Controls Verification

Verify that critical technical controls are actually working — not just configured on paper. Test before an assessor does.

## TECHNICAL VERIFICATION CHECKLIST

| | | |
|---|---|---|
| ■ | ★★★ **MFA is Enforced** | Tested: attempted login without MFA is blocked. Conditional Access policy tested in report-only mode first. |
| ■ | ★★★ **Account Lockout Works** | Tested: 5-10 failed login attempts triggers lockout. Verified on all systems including VPN and M365. |
| ■ | ★★★ **Login Banner Displays** | Tested: login banners appear on all systems before authentication. Screenshots captured. |
| ■ | ★★★ **Session Lock Activates** | Tested: screens lock after ≤15 minutes of inactivity on all workstations and laptops. Cannot be disabled by users. |
| ■ | ★★★ **VPN Split Tunneling Disabled** | Tested: while on VPN, all internet traffic routes through the tunnel. Verified with IP leak test. |
| ■ | ★★★ **USB Blocking Works** | Tested: unauthorized USB storage device is blocked when connected. Audit event is generated. |
| ■ | ★★★ **Antivirus Real-Time Protection On** | Verified on all systems via centralized dashboard. No systems with disabled or outdated AV. |
| ■ | ★★★ **BitLocker / Encryption Active** | Verified on all laptops via BitLocker management report or Intune compliance. 100% encrypted. |
| ■ | ★★★ **Firewall Default-Deny Confirmed** | Firewall rule review completed. Default-deny posture confirmed. Unnecessary rules removed. |
| ■ | ★★☆ **FIPS Mode Enabled** | Windows FIPS mode enabled via Group Policy on all systems. Verified via registry or GPO report. |
| ■ | ★★☆ **NTP Synchronization Verified** | All systems syncing to authoritative NTP source. Time drift within acceptable range across all systems. |
| ■ | ★★☆ **Legacy Protocol Disabled** | TLS 1.0, 1.1, SSL disabled. SMBv1 disabled. NTLMv1 disabled. Verified via SSL Labs or IIS Crypto tool. |
| ■ | ★☆☆ **Vulnerability Scan Run** | Vulnerability scan completed within last 30 days. All critical/high findings remediated or in POA&M.; |

## DOMAIN 4 — People & Process

Assessors interview personnel and observe processes — not just review documentation. Your team must know their security responsibilities.

| PEOPLE & PROCESS CHECKLIST | | |
|---|---|---|
| ■ | ★★★ **Key Personnel Identified** | System Owner, ISSO, IT Admin, and Incident Response Lead are identified and know their roles. |

| | | |
|---|---|---|
| ■ | ★★★ **Team Briefed on Assessment** | All relevant staff briefed on the assessment process, what assessors will ask, and their role in demonstrating compliance. |
| ■ | ★★★ **Offboarding Process Tested** | Verified: a simulated employee departure results in complete access revocation within 24 hours across all systems. |
| ■ | ★★★ **Incident Response Tested** | Tabletop exercise completed within last 12 months. DoD 72-hour reporting procedure is known by IR lead. |
| ■ | ★★★ **Security Training Current** | All employees have completed annual security awareness training. Records on file. |
| ■ | ★★☆ **Insider Threat Team Exists** | Cross-functional insider threat team (HR + IT + management) formally designated in writing. |
| ■ | ★★☆ **Visitor Control Practiced** | All employees know the visitor escorting requirement. Visitor log is being consistently maintained. |
| ■ | ★☆☆ **Background Checks Current** | Background check records on file for all personnel with CUI access. No gaps for recent hires. |

## DOMAIN 5 — Scope & Boundary Definition

An inaccurate or incomplete scope definition is one of the most common C3PAO assessment failures. If assets are in scope but not documented, all related controls are findings.

| SCOPE & BOUNDARY CHECKLIST | | |
|---|---|---|
| ■ | ★★★ **CUI Boundary is Documented** | Written CUI boundary statement in SSP Section 1. Clearly defines what is in scope and what is out of scope. |
| ■ | ★★★ **Network Diagram is Accurate** | Network diagram matches actual infrastructure. Walk the diagram — verify every device is accounted for. |
| ■ | ★★★ **Cloud Services Documented** | All cloud services handling CUI listed (M365, SharePoint, OneDrive, backup, etc.). ISAs in place for each. |
| ■ | ★★★ **Remote Work Sites Covered** | Remote/home office locations where CUI is accessed are addressed in SSP Section 5. VPN required and enforced. |
| ■ | ★★★ **Mobile Devices Covered** | All mobile devices with CUI access are enrolled in MDM and listed in asset inventory. |
| ■ | ★★☆ **Third-Party Access Documented** | All MSP, vendor, and contractor access to CUI systems is documented with ISAs. |
| ■ | ★★☆ **No Scope Creep** | Verify no systems handle CUI that are not in the documented scope. Walk the office and ask staff. |

| | | |
|---|---|---|
| ☐ | ★☆☆ **CUI Data Flow Mapped** | Data flow diagram showing how CUI enters, moves through, and exits the organization. Documented in SSP. |

## DOMAIN 6 — SPRS Submission Readiness

Before submitting to SPRS, verify all prerequisites are in place. A failed or inaccurate SPRS submission creates legal risk and may delay contract awards.

| SPRS SUBMISSION CHECKLIST | | |
|---|---|---|
| ☐ | ★★★ **SAM.gov Registration Active** | Company SAM.gov registration is current and active. CAGE code matches contract. Verify at sam.gov. |
| ☐ | ★★★ **SPRS Account Accessible** | Authorized person has tested login to sprs.csd.disa.mil. DS Logon credentials are working. |
| ☐ | ★★★ **Score is Calculated** | SPRS score calculated using official DoD methodology (WB5). Score reflects actual implementation status. |
| ☐ | ★★★ **Score is Accurate** | Score matches what WB3 gap assessment shows. No controls marked Met in SPRS that are actually Not Met. |
| ☐ | ★★★ **Senior Official Available** | Authorizing Official (owner, CEO, or authorized officer) is available and willing to submit the affirmation. |
| ☐ | ★★★ **Affirmation Language Reviewed** | Senior official has read the affirmation statement (32 CFR Part 170). Understands the False Claims Act implications. |
| ☐ | ★★★ **POA&M; Submitted if Applicable** | If submitting with open POA&M; items, all items are documented in WB5 with 180-day-compliant target dates. |
| ☐ | ★★☆ **Confirmation Number Plan** | Process in place to record and retain SPRS confirmation number immediately after submission. |
| ☐ | ★★☆ **Renewal Date Calendared** | Annual renewal date (12 months from submission) is recorded in WB2/WB3 tracker and on calendar. |

## DOMAIN 7 — C3PAO Assessment Readiness (Third-Party Only)

If pursuing third-party CMMC Level 2 certification (required for most CUI contracts by November 2026), these additional items must be in place before the assessment begins.

| C3PAO ASSESSMENT CHECKLIST | | |
|---|---|---|
| ☐ | ★★★ **C3PAO Selected & Scheduled** | A DoD-authorized C3PAO has been selected from the Cyber AB Marketplace (cyberab.org). Assessment scheduled. |

| | | |
|---|---|---|
| ■ | ★★★ **CMMC-AB Marketplace Verified** | Verify C3PAO is currently authorized at cyberab.org/marketplace. Do not use unverified assessors. |
| ■ | ★★★ **Assessment Scope Agreed** | Scope of assessment formally agreed with C3PAO. Matches your documented CUI boundary. |
| ■ | ★★★ **Pre-Assessment Package Ready** | SSP, network diagram, asset inventory, and POA&M; ready to share with C3PAO before assessment begins. |
| ■ | ★★★ **Evidence Repository Accessible** | Evidence folder is organized, complete, and can be shared securely with the assessment team. |
| ■ | ★★★ **Interview Subjects Identified** | Personnel available for assessor interviews: System Owner, IT Admin, ISSO, and general users. |
| ■ | ★★☆ **Assessment Contract Signed** | Legal contract with C3PAO includes scope, timeline, deliverables, and confidentiality protections. |
| ■ | ★★☆ **Remediation Window Planned** | If findings are expected, time is allocated post-assessment for remediation before certification deadline. |
| ■ | ★★☆ **Budget Confirmed** | Assessment cost, any remediation costs, and certification fees are budgeted and approved. |
| ■ | ★☆☆ **Mock Assessment Conducted** | Internal mock assessment or pre-assessment readiness review completed using this checklist. |

■ **Note**

This domain applies only to organizations pursuing C3PAO third-party certification. For self-assessment SPRS submissions, skip to Domain 8.

## DOMAIN 8 — Common Assessment Failure Points

These are the most frequently cited deficiencies in CMMC Level 2 assessments, based on DoD assessment methodology guidance and industry experience. Check each one carefully.

| COMMON FAILURE POINTS CHECKLIST | | |
|---|---|---|
| ■ | ★★★ **SSP Matches Reality** | The SSP describes what is ACTUALLY implemented — not what you plan to implement. Assessors verify every SSP statement against evidence. |
| ■ | ★★★ **No Shared Accounts** | Every user has a unique, individual account. No shared logins, no generic accounts used for real work. |
| ■ | ★★★ **Admin Rights are Restricted** | Standard users do not have local admin rights. IT staff use separate admin accounts for admin tasks only. |

| | | |
|---|---|---|
| ■ | ★★★ **MFA Cannot Be Bypassed** | MFA is enforced via Conditional Access — not just enabled as optional. Legacy authentication protocols are blocked. |
| ■ | ★★★ **Logs are Actually Reviewed** | Audit logs are not just collected — someone actually reviews them on a defined schedule. Review records exist. |
| ■ | ★★★ **Patch SLAs are Being Met** | Critical patches applied within 15 days. Evidence shows patches are being applied — not just that auto-update is on. |
| ■ | ★★★ **Offboarding is Immediate** | Terminated employees have access revoked same day. Records prove this — not just a policy that says it. |
| ■ | ★★★ **POA&M; is Credible** | POA&M; items have specific, realistic target dates within 180 days. Vague entries ("will fix later") fail assessments. |
| ■ | ★★☆ **Remote Access is Controlled** | No direct RDP from internet. All remote access through VPN with MFA. Split tunneling disabled. |
| ■ | ★★☆ **Backup is Encrypted and Tested** | Backups of CUI are encrypted. Restoration has been tested within last 12 months. |
| ■ | ★★☆ **Vendor Access is Monitored** | MSP/vendor remote sessions are monitored in real time. Sessions are logged. Sessions terminate after work is complete. |
| ■ | ★☆☆ **Guest WiFi is Separated** | Guest wireless network is on a separate SSID and VLAN from business/CUI network. No bridge between them. |

## DOMAIN 9 — Final Readiness Gate

Complete this final gate only after working through Domains 1–8. Every item below must be confirmed before proceeding.

| FINAL READINESS GATE | | |
|---|---|---|
| ■ | ★★★ **All Domain 1-8 Critical Items Checked** | Every ★★★ item across all domains is checked. No exceptions. |
| ■ | ★★★ **SPRS Score is Final and Accurate** | Score in WB5 reflects the true implementation state. Senior official has reviewed and agrees. |
| ■ | ★★★ **SSP is Final and Approved** | SSP has been reviewed, approved (signed) by the Authorizing Official, and version-controlled. |
| ■ | ★★★ **No Known Material Gaps Remain Undocumented** | Any remaining gaps are documented in the POA&M.; Nothing is hidden or omitted. |
| ■ | ★★★ **Legal Counsel Consulted (Recommended)** | Qualified legal counsel has reviewed the affirmation language and FCA implications. Especially if POA&M; items exist. |

| | | |
|---|---|---|
| ■ | **★★★ Senior Official Ready to Affirm** | Authorizing Official is available, has reviewed the SSP and score, and is prepared to submit the affirmation. |
| ■ | **★★★ All Records Retained** | Complete assessment package (SSP, evidence, POA&M;, this checklist) is saved and will be retained for contract duration + 3 years. |

## DOMAIN 10 — Assessment Sign-Off

Complete this sign-off section after all checklist items are reviewed. The signatures below attest that the organization has completed the pre-assessment readiness review in good faith and is prepared to proceed.

| | |
|---|---|
| **Assessment Type:** | ■ Self-Assessment (SPRS Submission) ■ C3PAO Third-Party Assessment |
| **Checklist Completed By:** | _____ |
| **Title:** | _____ |
| **Date Completed:** | _____ |
| **Critical Items Checked:** | ___ of ___ Critical (★★★) items confirmed |
| **Important Items Checked:** | ___ of ___ Important (★★■) items confirmed |
| **Open Issues Noted:** | _____ |
| | |
| **Authorizing Official Name:** | _____ |
| **Title:** | _____ |
| **Signature:** | _____ |
| **Date:** | _____ |
| **Affirmation:** | ■ I confirm this organization is ready to proceed with the above assessment type. |

*This checklist is an educational tool and does not guarantee CMMC compliance or certification. Retain this completed checklist with your assessment records for the duration of your contract plus three years. Re-complete this checklist for each annual renewal and before any C3PAO assessment.*