AMERIFUSIONGOVCON · FEDERAL COMPLIANCE PRACTICE

The 12 CMMC Level 2 Documentation Gaps That Fail Most C3PAO Assessments

A free guide for defense contractors handling CUI. The 12 documentation gaps that fail most C3PAO assessments and how to close each one before the formal review.

Josef Kamara

CPA · CISSP · CISA

15+ years in audit and risk · Former KPMG, BDO, Stryker

AmerifusionGovCon · amerifusiongovcon.com

v1.0 · May 2026

Table of Contents

Why this guide. C3PAO assessors fail defense contractors on documentation more often than on technology. The pattern is consistent across DCMA DIBCAC High Assessments and the early CMMC Level 2 C3PAO assessments running under 32 CFR Part 170 Phase 1, which took effect November 10, 2025. Tooling exists. The documentation that proves the tooling is doing what the System Security Plan claims it does, does not.

How to read it. Twelve gaps, two per NIST SP 800-171 Rev 2 family across the six families that produce the highest finding rates: Access Control (AC), Identification and Authentication (IA), Audit and Accountability (AU), Configuration Management (CM), System and Communications Protection (SC), and System and Information Integrity (SI). Each gap follows the same structure: the documentation that fails, why C3PAOs cite it, and how to close it before the formal review.

Citations reference primary sources at `acquisition.gov`, `ecfr.gov`, `csrc.nist.gov`, and `dodcio.defense.gov`. This guide is current as of May 2026 and reflects DFARS Class Deviation 2024-O0013 (which keeps the assessment basis on Rev 2) and the four-phase CMMC rollout finalized in 88 FR / DFARS Final Rule, Sept 10, 2025.

AC

Access Control

NIST 800-171 REV 2 FAMILY 3.1 · 22 CONTROLS

GAP 01 · AC.L2-3.1.1 / AC.L2-3.1.2

The account inventory and role/permission matrix

DOCUMENTATION THAT FAILS

The SSP states that access is granted on a least-privilege basis and that accounts are reviewed periodically. The assessor asks for the current list of every account in the CUI environment, the role each account holds, and the date each role was last reviewed. There is no list. Or the list exists for the on-premises Active Directory but not for the Microsoft 365 GCC High tenant, the AWS GovCloud organization, the EDR console, the build pipeline, or the third-party DLP service.

WHY C3PAOS CITE IT

NIST SP 800-171A objective 3.1.1[a] requires that authorized users are identified and that the system limits access to those users. Without an inventory, no one can tell what "authorized" means. NIST SP 800-171A objective 3.1.2[c] requires that system access is limited to the types of transactions and functions authorized users are permitted to execute. Without a role/permission matrix, that bound is unprovable. The control is one of the seventeen FAR 52.204-21 basic safeguarding controls and is weighted at 5 points in the DoD Assessment Methodology - the highest impact tier.

HOW TO CLOSE IT

1. Build a single account inventory across every system that processes, stores, or transmits CUI. Include identity provider exports (Entra ID, Okta, on-prem AD), SaaS admin console exports (M365, AWS, Salesforce, Atlassian), and locally-managed accounts.
2. Map every account to a role. Roles, not users, get the privileges. Document each role's permission set and the business justification.
3. Establish an access-review cadence - quarterly is the floor for privileged roles, semi-annually for the rest. Save the review record: reviewer, date, accounts retained, accounts removed.
4. Tie the inventory to the SSP. The SSP describes how access is provisioned, reviewed, and revoked; the inventory and review records are the evidence.

Sources: NIST SP 800-171 Rev 2 §3.1.1, 3.1.2 · NIST SP 800-171A Assessment Procedures · DoD Assessment Methodology v1.2.1 Table 1

GAP 02 · AC.L2-3.1.5 / AC.L2-3.1.6 / AC.L2-3.1.7

Privileged-account separation evidence

DOCUMENTATION THAT FAILS

The same identity is a domain administrator, a Microsoft 365 Global Administrator, the EDR console root, and the user the IT lead reads email with. The SSP says the contractor "follows least privilege." There is no documented separation between privileged identities and the everyday accounts those people use. There is no record of which privileged accounts exist, who holds them, or when they were last used.

WHY C3PAOS CITE IT

The 800-171 Rev 2 controls 3.1.5 (employ the principle of least privilege), 3.1.6 (use non-privileged accounts when accessing non-security functions), and 3.1.7 (prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs) read together as a single requirement: privileged identities exist, they are separate from everyday identities, their use is logged, and the log is reviewed. NIST SP 800-171A 3.1.5[d] and 3.1.7[c] both expect documentation of which functions are privileged and audit records of their execution. Generic, shared, or undocumented admin accounts fail all three.

HOW TO CLOSE IT

1. Inventory every privileged account separately. For each, name the human who holds it, the privileged functions it enables, and the systems it controls.
2. Issue separate privileged identities (e.g., `jdoe-adm@contoso.us`) distinct from each user's everyday account. The everyday account does daily work; the privileged account does admin work.
3. Log privileged-function execution. Forward to the SIEM. Define an alerting rule on use of any account in the privileged inventory from outside an admin workstation, off-hours, or from an unexpected source.
4. Document the privileged-functions list in the SSP and reference it from the audit/review section. Maintain a quarterly review record showing each privileged account is still required.

Sources: NIST SP 800-171 Rev 2 §3.1.5, 3.1.6, 3.1.7 · NIST SP 800-171A objectives 3.1.5[a-d], 3.1.7[a-c]

IA Identification and Authentication

NIST 800-171 REV 2 FAMILY 3.5 · 11 CONTROLS

GAP 03 · IA.L2-3.5.3

Multi-factor authentication coverage evidence

DOCUMENTATION THAT FAILS

The MFA policy is on file and clearly written. The SSP claims MFA is required for all privileged accounts and for network access to non-privileged accounts. The assessor asks for the configuration export that proves it - the conditional-access policy from Entra ID, the MFA enforcement settings from Okta, the per-application policy from Duo - plus an authentication log sample showing MFA was prompted and satisfied for a representative privileged login. The contractor produces neither.

WHY C3PAOS CITE IT

3.5.3 is one of the 5-point controls under the DoD Assessment Methodology - a single missing control of this weight drops the SPRS score from +110 to +105 and shifts the closeout calculus. NIST SP 800-171A objectives 3.5.3[a-c] require evidence that MFA is enforced both for local and network access to privileged accounts and for network access to non-privileged accounts. Policy text alone does not satisfy any of the three objectives. The DCMA DIBCAC field experience is consistent: the gap is rarely "no MFA;" it is "no proof of MFA coverage." Every external-facing entry point - VPN, web mail, M365 portal, RDP, jump hosts, console access to GovCloud - must be in scope and demonstrable.

HOW TO CLOSE IT

1. Build an MFA coverage matrix. Columns: entry point, identity provider, MFA method (FIDO2, TOTP, push, SMS-not-acceptable-for-CUI), enforcement scope (all users / privileged only / conditional), evidence reference.
2. Export the configuration that enforces MFA at each entry point. Save as a dated screenshot or CLI export, not a policy document.
3. Pull a 30-day authentication log sample for at least one privileged user and one non-privileged remote login. Demonstrate the MFA challenge in the log.
4. Document the matrix in the SSP under 3.5.3 and reference the evidence files. Re-run the matrix after any change to identity infrastructure.

Sources: NIST SP 800-171 Rev 2 §3.5.3 · NIST SP 800-171A objectives 3.5.3[a-c] · DoD Assessment Methodology v1.2.1 (5-point control)

GAP 04 · IA.L2-3.5.7 / 3.5.8 / 3.5.9 / 3.5.10

Password policy implementation proof

DOCUMENTATION THAT FAILS

The contractor's information security policy describes password complexity, history, lockout, and storage requirements. The Group Policy Object on the domain, the Entra ID password protection policy, and the SaaS-specific password rules each say something slightly different. The SSP describes the policy. It does not describe the in-effect technical control. The assessor asks for the GPO export, the Entra ID policy export, and the SaaS-by-SaaS configuration. The result is a set of inconsistencies that contradict the policy document.

WHY C3PAOS CITE IT

3.5.7 (minimum password complexity), 3.5.8 (password history), 3.5.9 (allow temporary password use only with immediate change), and 3.5.10 (cryptographically protect passwords at rest and in transit) read as a cluster: a written policy that is not technically enforced everywhere is not a control. Each of the four maps to specific assessment objectives in NIST SP 800-171A that look for both policy text and technical evidence. The cluster is a frequent C3PAO partial-credit area where contractors get scored as "not implemented" because the implementation does not match the documentation.

HOW TO CLOSE IT

1. Run a configuration sweep across every identity store: on-prem AD, Entra ID, every CUI-relevant SaaS, every privileged-access tool, every developer service. Document the in-effect setting for complexity, history, lockout, and storage.
2. Reconcile the configuration to the policy. Where the configuration is weaker, change the configuration. Where the policy is wrong, update the policy. Same answer in both places.
3. For systems that cannot enforce the full policy technically, document the compensating control (e.g., FIDO2 keys instead of passwords) and reference it in the SSP.
4. Save the configuration evidence in a single, dated location. Re-run the sweep before each annual SSP review.

Sources: NIST SP 800-171 Rev 2 §3.5.7-3.5.10 · NIST SP 800-63B (referenced for digital identity guidance)

AU Audit and Accountability

NIST 800-171 REV 2 FAMILY 3.3 · 9 CONTROLS

GAP 05 · AU.L2-3.3.1 / AU.L2-3.3.2

The audit log coverage matrix

DOCUMENTATION THAT FAILS

"We log everything to the SIEM." The assessor asks which systems forward which event types, where the logs are stored, how long they are retained, how integrity is preserved, and how access to the log store is itself audited. There is no documented matrix. The SSP describes the SIEM in the abstract. There is no evidence that a specific event class - say, privileged authentication or configuration change on a domain controller - is captured, parsed, retained, and reviewable.

WHY C3PAOS CITE IT

3.3.1 requires the contractor to create and retain audit records to enable monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 requires audit record content sufficient to ensure that actions can be traced to individual users. NIST SP 800-171A objectives 3.3.1[a-c] expect a documented inventory of event types, retention periods, and protections. Sampling failure is the typical pattern: the assessor selects three event types from the SSP - for example, account lockout, file integrity change, and EDR detection - and asks to see one of each from the last 30 days. If any are missing or unretrievable, both controls score as not-implemented.

HOW TO CLOSE IT

1. Build an audit log coverage matrix. Columns: system, event types, log destination, retention period, integrity protection (immutable storage / WORM / external SIEM), review cadence, access control on the log store.
2. Run a sampling exercise on the matrix yourself, before the assessor does. Pull three event types per system from the last 30 days and confirm they are retrievable.
3. Document the matrix as an SSP appendix. Update on each environment change.
4. For systems that cannot forward logs natively, document the alternate capture method (agent, syslog forwarder, API export) and the gap window if any.

Sources: NIST SP 800-171 Rev 2 §3.3.1, 3.3.2 · NIST SP 800-92 (log management guidance) · NIST SP 800-171A objectives 3.3.1[a-c], 3.3.2[a-b]

GAP 06 · AU.L2-3.3.3 / AU.L2-3.3.5

Audit log review evidence

DOCUMENTATION THAT FAILS

The SIEM exists. The review records do not. The assessor asks for the last 90 days of review tickets, the alerting rules with thresholds, and a sample of escalations. The contractor produces a screenshot of the SIEM dashboard. That is not evidence of review. A SIEM with no review history is logging in name only.

WHY C3PAOS CITE IT

3.3.3 requires the contractor to review and update the logged events to enable monitoring of what the organization defines as significant. 3.3.5 requires the contractor to correlate audit record review, analysis, and reporting processes for investigation. NIST SP 800-171A objectives expect three pieces: a defined event taxonomy (what gets reviewed daily / weekly / on-demand), evidence of review actually occurring (tickets, summaries, on-call escalations), and an alerting ruleset that maps to the defined taxonomy. The control is not "we have logs." It is "we read them."

HOW TO CLOSE IT

1. Define the event taxonomy in writing. What is reviewed daily (failed-MFA spikes, privilege escalations, EDR critical alerts), weekly (account inventory deltas, GPO changes), monthly (firewall rule diffs).
2. Save the alerting ruleset. Each rule should reference the taxonomy item it enforces and the threshold that triggers an alert.
3. Generate review records. A weekly review summary signed by the reviewer. Tickets in the ITSM system tied to alerts. Escalation records when alerts fire.
4. Retain 90 days of review evidence at minimum. Sample your own program before the assessor does.

Sources: NIST SP 800-171 Rev 2 §3.3.3, 3.3.5 · NIST SP 800-171A objectives 3.3.3[a-b], 3.3.5[a-c]

CM

Configuration Management

NIST 800-171 REV 2 FAMILY 3.4 · 9 CONTROLS

GAP 07 · CM.L2-3.4.1 / CM.L2-3.4.2

Baseline configuration documentation

DOCUMENTATION THAT FAILS

The contractor has hardening guides from when the environment was built. They have not been refreshed against what is actually deployed. The SSP says "we follow CIS Benchmarks" without naming the benchmark version, the system class it applies to, or the deviation register. The assessor asks for the current documented baseline for workstations, servers, network devices, and cloud services. The result is a stale guide and a current environment that has drifted.

WHY C3PAOS CITE IT

3.4.1 requires the contractor to establish and maintain baseline configurations and inventories of organizational systems. 3.4.2 requires the contractor to establish and enforce security configuration settings for IT products in those systems. NIST SP 800-171A 3.4.1[a-c] expects a current baseline per system class, an inventory tied to that baseline, and evidence the baseline is enforced. "Current" is the operative word. A 2023 baseline against a 2026 environment is a not-implemented finding.

HOW TO CLOSE IT

1. Per system class, document the baseline. Reference a public benchmark (CIS, DISA STIG, vendor hardening guide) by version. Maintain a deviation register naming each setting that intentionally differs.
2. Implement automated drift detection. Microsoft Defender for Cloud, AWS Config, Tenable, Tanium, or open-source equivalents all generate the evidence.
3. Tie drift detection results to a remediation workflow with an SLA per severity tier.
4. Refresh the baseline document on a defined cadence - annual at minimum, plus on each material environment change.

Sources: NIST SP 800-171 Rev 2 §3.4.1, 3.4.2 · NIST SP 800-171A objectives 3.4.1[a-c], 3.4.2[a-b] · CIS Benchmarks, DISA STIGs (commonly referenced sources)

GAP 08 · CM.L2-3.4.3 / CM.L2-3.4.5

Change control records

DOCUMENTATION THAT FAILS

The contractor uses ServiceNow, Jira, or another change ticketing system. The SSP says "all changes go through change management." The assessor samples five recent production changes and asks to see, for each, the approval, the test result, the deployment record, and the post-implementation review. Two of the five are missing the test result. One was deployed before the approval. One has no post-implementation review. None of the five connects the ticket back to the actual configuration change in production.

WHY C3PAOS CITE IT

3.4.3 requires the contractor to track, review, approve or disapprove, and log changes to organizational systems. 3.4.5 requires the contractor to define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. The cluster looks for closed-loop evidence: ticket -> approval -> test -> deploy -> verify -> close. A ticketing tool without that closed loop produces tickets, not change control. Sampling exposes the gap quickly.

HOW TO CLOSE IT

1. Define what counts as a "change" in writing - infrastructure-as-code merge, GPO edit, firewall rule change, identity-provider policy change, SaaS admin setting.
2. Require approval on the ticket before deploy. Block deployment workflows on ticket state where possible (CI/CD policy gate).
3. Require a test artifact attached to the ticket and a post-implementation review entry within 5 business days of deploy.
4. Document the workflow in the SSP. Pull a quarterly sample of 10 changes and verify the closed loop. Save the sampling record.

Sources: NIST SP 800-171 Rev 2 §3.4.3, 3.4.5 · NIST SP 800-171A objectives 3.4.3[a-d], 3.4.5[a-d]

SC

System and Communications Protection

NIST 800-171 REV 2 FAMILY 3.13 · 16 CONTROLS

GAP 09 · SC.L2-3.13.1 / SC.L2-3.13.5

Network and CUI boundary diagram

DOCUMENTATION THAT FAILS

The SSP describes the boundary in prose. There is no current data-flow diagram. The most recent network diagram is from the original deployment. The actual firewall rule set, ACLs in the cloud VPCs, M365 conditional access policies, and SaaS allow-lists do not match what the SSP describes. The contractor cannot answer the question "where does CUI cross the boundary, and how is it controlled at each crossing?"

WHY C3PAOS CITE IT

3.13.1 requires the contractor to monitor, control, and protect communications at the external boundaries and key internal boundaries of the system. 3.13.5 requires implementation of subnetworks for publicly accessible system components, physically or logically separated from internal networks. NIST SP 800-171A 3.13.1[a-d] expects a defined boundary, identified communications, and protective measures at each. Mismatches between SSP and ACLs are the single most common SC finding category in the DCMA DIBCAC field experience. The gap is most often a boundary diagram that has not kept pace with cloud migration, SaaS adoption, or remote-work expansion.

HOW TO CLOSE IT

1. Produce a current data-flow diagram. Show every place CUI enters, transits, or leaves the boundary - email, file share, SaaS, cloud, contractor laptop, mobile device, third-party connection.
2. Tie each crossing to a control: firewall rule, conditional access policy, DLP rule, FIPS-validated VPN tunnel, FedRAMP-Moderate-equivalent CSP.
3. Cross-reference the diagram against the actual configuration. ACLs, conditional access policies, DLP rules. Reconcile.
4. Document the boundary and the diagram in the SSP. Update on every material network change.

Sources: NIST SP 800-171 Rev 2 §3.13.1, 3.13.5 · NIST SP 800-171A objectives 3.13.1[a-d], 3.13.5[a-c]

GAP 10 · SC.L2-3.13.11

FIPS-validated cryptography evidence

DOCUMENTATION THAT FAILS

The SSP states "all CUI is encrypted at rest and in transit using FIPS-validated cryptography." The assessor asks for the cryptographic inventory - every place CUI is encrypted, the module providing the algorithm, and the FIPS 140-2 or 140-3 validation certificate number from the NIST CMVP database. The contractor produces a sentence. Or BitLocker is enabled with FIPS mode disabled. Or OpenSSL is in use with a non-FIPS provider. Or a TLS configuration accepts non-validated cipher suites.

WHY C3PAOS CITE IT

3.13.11 is a 5-point control. The DoD Assessment Methodology weights it at the highest impact tier because cryptographic protection is the technical floor under the entire CUI handling regime. NIST SP 800-171A 3.13.11[a-b] requires the contractor to identify the cryptographic uses requiring FIPS-validated cryptography and to verify the cryptographic modules in use are validated. "Validated" has a specific meaning: a certificate number that resolves on the NIST Cryptographic Module Validation Program. Cryptography "in use" without a certificate reference is not validated cryptography. FIPS mode disabled in BitLocker invalidates the BitLocker validation. Non-FIPS OpenSSL providers invalidate the OpenSSL validation.

HOW TO CLOSE IT

1. Build a cryptographic inventory. Per protected location, name the module, the algorithm, and the FIPS validation certificate ID.
2. Verify each certificate on the CMVP database. Save the verification screenshot.
3. Confirm FIPS mode where required. BitLocker FIPS mode, Windows FIPS-enabled cryptography, Linux FIPS kernel, FIPS-mode OpenSSL provider, FIPS-mode TLS policy.
4. Document the inventory as an SSP appendix. Refresh on each upgrade of the underlying module.

Sources: NIST SP 800-171 Rev 2 §3.13.11 · NIST CMVP database (csrc.nist.gov) · FIPS 140-2 / 140-3 validation program · DoD Assessment Methodology v1.2.1 (5-point control)

SI

System and Information Integrity

NIST 800-171 REV 2 FAMILY 3.14 · 7 CONTROLS

GAP 11 · SI.L2-3.14.1 / SI.L2-3.14.4

Vulnerability management cadence

DOCUMENTATION THAT FAILS

"We run monthly vulnerability scans" appears in the policy. The assessor asks for the last 90 days of scan reports, the severity-tiered remediation SLAs, and closeout verification on a sample of findings. The contractor produces three scan reports with no remediation tracking, or scans that do not cover the full asset inventory, or a tooling stack (e.g., EDR + cloud security posture) that is producing findings nobody is closing.

WHY C3PAOS CITE IT

3.14.1 requires the contractor to identify, report, and correct system flaws in a timely manner. 3.14.4 requires update of malicious code protection mechanisms when new releases are available. NIST SP 800-171A 3.14.1[a-c] expects three things: a process to identify flaws, a process to correct them, and "timely" defined in writing. "Timely" is contractor-defined but must be defensible - a 365-day SLA on a critical vulnerability does not survive a sampling exercise. The control is also about coverage: if the scanner does not see the GovCloud workload, the workload is not in the program.

HOW TO CLOSE IT

1. Define a vulnerability management policy with severity-tiered SLAs. Industry-defensible windows: critical 14 days, high 30 days, medium 60-90 days, low at next quarterly cycle.
2. Confirm scanner coverage against the asset inventory. Network scanner, agent scanner, cloud security posture, container scanner, SaaS-side scanner.
3. Track remediation in a system that produces evidence: ticket, owner, closeout date, verification scan.
4. Save scan reports for at least 90 days. Pull a sample of recent critical findings and prove closeout against the SLA.

Sources: NIST SP 800-171 Rev 2 §3.14.1, 3.14.4 · NIST SP 800-171A objectives 3.14.1[a-c], 3.14.4[a-b] · CISA Known Exploited Vulnerabilities catalog (commonly used for prioritization)

GAP 12 · SI.L2-3.14.2

Flaw remediation tracking

DOCUMENTATION THAT FAILS

Patches go out via Intune, WSUS, Chef, Ansible, or a managed-service provider. The audit trail does not connect each CVE to a specific asset, a deployment date, and proof the SLA tier was met. The assessor samples three CVEs - one critical, one high, one medium - and asks for the deployment evidence and closeout verification. The result is a patch-management dashboard with aggregate compliance rates and no per-CVE traceability.

WHY C3PAOS CITE IT

3.14.2 requires the contractor to provide protection from malicious code at designated locations within organizational systems. Read with 3.14.1 (flaw remediation), the cluster requires evidence that flaws are closed - not just that a patching tool exists. NIST SP 800-171A 3.14.2[a-c] expects identification of designated locations, the protection mechanism in use, and evidence of update. Sampling exposes the gap when an aggregate "98% compliant" dashboard cannot answer "show me the deployment record for CVE-2025-XXXX on host SERVER-014."

HOW TO CLOSE IT

1. Maintain a CVE-to-asset traceability record. Most patching tools produce this if configured for per-CVE reporting; if yours does not, supplement with vulnerability scan correlation.
2. For each closed CVE, retain the deployment timestamp, the asset list, and the post-deployment verification scan confirming the CVE no longer detects.
3. For exceptions (legacy systems, vendor-blocked patches), document the compensating control and the risk acceptance with named approver and review date.
4. Sample your own program. Pick three recent critical CVEs at random and walk the trail before an assessor does.

Sources: NIST SP 800-171 Rev 2 §3.14.2 · NIST SP 800-171A objectives 3.14.2[a-c]

About the author · How to use this guide

CLOSING NOTES · CITATIONS · WHERE TO GO NEXT

I am Josef Kamara - a CPA, CISSP, and CISA with fifteen-plus years of audit and risk experience across **KPMG**, **BDO**, and **Stryker**. At BDO, I led both the third-party attestation practice (SOC 1, SOC 2, HIPAA, HITRUST) and the information assurance team. At Stryker, I managed the IT audit function across a regulated medical-device manufacturer with substantial federal and contract exposure. I founded **Amerifusion GovCon** at amerifusiongovcon.com to deliver clause-level federal compliance work to defense contractors and agency program offices. I run CMMC readiness assessments for a small number of contractors per quarter.

This guide is the documentation-readiness checklist I would hand a defense contractor at the start of a CMMC Level 2 readiness engagement. The 12 gaps are the patterns I see most often when the SSP describes one program and the actual environment runs another. Closing them before the formal review is not a heavier lift than the work the contractor has already done - it is a smaller lift. It is the work of writing down, with evidence, what the team is already doing, and then fixing the small set of places where the writing does not match the doing.

How to use what you have just read

1. **Triage by 5-point controls first.** Gaps 03 (MFA evidence) and 10 (FIPS cryptography) are the highest-impact items. A single missed 5-point control is the same five-point swing in the SPRS score as five missed 1-point controls.
2. **Sample your own program before the assessor does.** Each "How to close it" section ends with a self-sampling exercise. Run those before the formal review. The findings you generate are easier to fix than the ones a C3PAO generates with billing attached.
3. **Reconcile the SSP after every fix.** Documentation gaps close when the SSP describes the actual program and the evidence file resolves when sampled. Anything else is a fix that did not finish.
4. **Build the package once, well.** The supporting documentation that holds up under a C3PAO review is the same documentation that holds up under a prime contractor's flow-down request. Most contractors build it twice; the work is to build it once.

- Josef Kamara
CPA · CISSP · CISA

Ready to pressure-test your documentation?

Amerifusion GovCon delivers CMMC Level 2 readiness assessments and SSP / POA&M build engagements for defense contractors. Bring us the SSP, the assessment workbook, and the POA&M you have today. We tell you what survives a C3PAO review, and what does not.

Schedule a CMMC readiness consultation →

Citations. DFARS 252.204-7012 · 7019 · 7020 · 7021 · 7025 · NIST SP 800-171 Rev 2 · NIST SP 800-171A · DoD Assessment Methodology v1.2.1 · 32 CFR Part 170 (CMMC Program Rule) · NIST CMVP · DoD CIO CMMC home.