CMMC Readiness Spot Check

These are the most common areas where certified assessors identify issues during CMMC Level 2 assessments. Use this spot-check to validate that your program is grounded, documented, and ready for formal review.

1. CUI Boundary Clarity

☐ We've clearly defined the CUI environment and documented system boundaries
☐ All in-scope systems and users are mapped without ambiguity
☐ Cloud environments (e.g., GCC High, AWS GovCloud) are properly segmented and justified

2. System Security Plan (SSP) Accuracy

☐ Our SSP is current and specific to our implementation
☐ Each control includes detailed, evidence-based descriptions
☐ Shared responsibility controls (e.g., with cloud providers) are validated and included

3. Policy-to-Practice Alignment

☐ Policies exist for each family of controls — and are approved and accessible
☐ Procedures reflect actual technical configurations
☐ Staff can describe how they follow these policies in daily operations

4. Evidence Preparedness

☐ Evidence for each control has been collected and reviewed
☐ Screenshots, logs, or exports are timestamped and complete
☐ At least one internal mock or practice run has reviewed evidence under time constraints

5. Common Early Flags

☐ Inconsistent artifact formatting or vague control descriptions
☐ Use of "template" documents without tailoring
☐ Policies are in place, but not followed in practice

Next Step: If you're unsure about even one of these items — it's time for a readiness consultation. Coalfire Federal is a certified RPO and C3PAO and has helped numerous DIB organizations pass their CMMC assessments with clarity and confidence.