Redspin

CMMC RECERTIFICATION CHECKLIST

Your first certification is just the start. Here's what to do over the next 3 years to stay compliant, and what to check before recertification.

1 GOVERNANCE & OWNERSHIP

Pro Tip: *These are ongoing responsibilities, not an annual or ad hoc exercise*

□ Named CMMC Owners for all 14 NIST 800-171 domains
□ Defined executive accountability (Affirming Official understands liability)
□ Annual management review of CMMC posture
□ Compliance responsibilities included in role descriptions
□ Succession plan for key compliance roles (turnover mitigation)

Caution: Assessors routinely flag failures tied to staff turnover and unclear ownership at recertification.

2 SYSTEM SECURITY PLAN (SSP)

Pro Tip: *The SSP is a top recertification failure area*

□ SSP reviewed and updated at least annually
□ SSP updated after any:
- Infrastructure changes
- Cloud service changes
- New CUI contracts
- Network redesigns
- Security/IT governance updates

□ Asset inventory matches live environment
□ Data flow diagrams reflect actual CUI movement
□ Control implementations match technical reality (no template language)

Caution: SSP drift is one of the most common Level 2 recertification failures

3 SCOPE MANAGEMENT & BOUNDARY CONTROL

Pro Tip: *These will help you prevent silent (costly) scope creep*

□ Maintain current SSP and network/data flow diagrams reflecting the authorized CMMC assessment scope
□ Ensure diagrams and scope documentation include:
- ESPs/MSSPs/MSPs/CSPs
- Remote access pathways
- External interconnections and boundary systems
- CUI storage, processing, and transmission locations

□ Evaluate new tools, services, systems, and integrations for CUI impact and scope implications as part of configuration/change management processes
□ Periodically validate boundary protections and access controls to confirm only authorized users, systems, and services interact with the CUI environment

Caution: Misaligned scope is consistently cited as a primary assessment failure cause. A new assessment is required if there are significant architectural or boundary changes to the previous CMMC Assessment Scope.

4 EXTERNAL SERVICE PROVIDERS (ESPS)

Pro Tip: *Inherited controls must stay inherited, and you should make sure your CMMC and solution partners and solution are vetted!*

□ FedRAMP Moderate (or equivalent) status verified annually
□ Shared Responsibility Matrix documented and current
□ ESP responsibilities reflected in SSP
□ Licensing tier changes reviewed for compliance impact
□ Contracts retain compliance language

Caution: Contractors remain accountable and responsible even when controls are inherited

5 EVIDENCE COLLECTION & RETENTION

Pro Tip: *Emphasize proof and verifiability over process statements.*

□Centralized evidence repository maintained. Evidence retained for:
- Log reviews
- Vulnerability scans
- Patch management
- Risk assessments
- Access reviews

□ Evidence shows ongoing activity, not snapshots
□ Retention aligns with assessment lifecycle expectations

Caution: Evidence gaps, not missing controls, cause most recertification delays

6 CONFIGURATION & CHANGE MANAGEMENT

Pro Tip: *This is a high-weight findings area*

□ Approved system baselines documented
□ Configuration changes tracked and approved
□ Security impact analysis performed for changes
□ Patch cadence documented and followed
□ Privileged access reviewed regularly
□ Operational plan of action is updated regularly

Caution: Configuration drift is often discovered during technical validation

7 LOGGING, MONITORING & INCIDENT RESPONSE

Pro Tip: *This is where you must prove operational maturity (this is why re-certification is "harder")*

□ Logs collected and protected
□ Logs reviewed on a defined schedule
□ Types of logs captured and the content of those logs reviewed on a defined schedule
□ Alerts tested and validated
□ Incident Response Plan reviewed annually
□ Annual tabletop exercises conducted and documented
□ Lessons learned documented (a nice to have, not a requirement)

Caution: Assessors expect repeatable IR and monitoring, not one-time setup. This often results in a fail due to turnover.

8 TRAINING & AWARENESS

Pro Tip: *Role-based training gaps are common at recertification*

□ Training on security risks and governance is updated as needed
□ Annual security awareness training completed
□ Role-based training completed for personnel with information security-related duties
□ Insider threat awareness addressed
□ Training records retained
□ New hires trained before system access

Caution: This often results as a "fail" due to turnover

9 ANNUAL AFFIRMATION READINESS

Pro Tip: *Annual affirmations carry legal and contractual risk*

□ Re-validate applicable controls and evidence prior to affirmation
□ Assess and document any environmental or system changes
□ Brief the Affirming Official on current security posture, risks, and gaps before sign-off
□ Submit annual affirmation of continuous compliance in SPRS (required every year between your triennial C3PAO assessments)
□ Confirm CMMC certification status in SPRS is current and reflects Final Level 2
□ Verify SPRS record is accessible and accurate for prime contractors and contracting officers to review

Caution: A false or inaccurate affirmation submitted to SPRS can constitute a violation of the False Claims Act, creating personal legal liability for the Affirming Official and contractual risk for the organization.

BEST-PRACTICE CADENCE SUMMARY

SSP review	Scope validation	Evidence collection	Training	ESP review	IR tabletop	Management review
Annually + after changes	Annually	Continuous	Annually + onboarding	Annually	Annually	Annually

You passed once. Now prove you can sustain it.

CMMC Level 2 recertification occurs every three years. Annual SPRS affirmation is required every year in between.

SCAN TO CONTACT US

(888) 907-3335
info@redspin.com