NIST 800-171 & CMMC Level 2 Readiness Checklist + SPRS Scoring Cheat Sheet

The 24 program steps assessors actually look for, the official scoring weights, and the traps that cost contractors points. Built from real CMMC engagements by ITSECOPS — the CMMC specialists outside the US.

PHASE 1 — Scope & plan (weeks 1–2)

- ■ Identify where FCI and CUI actually live: systems, shares, mailboxes, SaaS, backups — and where they don't.
- ■ Decide enclave vs. enterprise scope. A well-designed enclave typically cuts cost 40–60%.
- ■ Classify your data: FCI only, CUI Basic, CUI-Specified, ITAR/EAR — this drives cloud requirements (commercial vs. FedRAMP Moderate vs. GCC High + US persons).
- ■ Inventory every asset in scope: hardware, software, cloud services, and the people who touch CUI.
- ■ Confirm your contractual clauses: DFARS 252.204-7012, 7019, 7020, 7021 — know which apply today.
- ■ Name an accountable owner (internal lead, vCISO, or RPO-guided program manager).

PHASE 2 — Technical controls (weeks 3–10)

- ■ MFA everywhere for local and network access to CUI systems and for all privileged accounts (3.5.3 — a 5-point control).
- ■ FIPS-validated cryptography protecting CUI at rest and in transit (3.13.11 — 5 points; 'FIPS-capable but not enabled' loses points).
- ■ Access control: least privilege, separation of duties, session lock, remote-access control.
- ■ Audit logging centralized and reviewed — SIEM or managed SOC with retention.
- ■ Endpoint protection, patching SLAs, and configuration baselines (CIS or DISA STIG aligned).
- ■ Encrypted, tested backups — restore drills documented, media protected.
- ■ Boundary protection: segmented networks, controlled interfaces, deny-by-default.
- ■ Incident response capability: plan, roles, reporting path incl. 72-hour DIBNet reporting for 7012.

PHASE 3 — Documentation & evidence (weeks 6–12)

- ■ System Security Plan (SSP) — without it 3.12.4 cannot score and your assessment cannot proceed.
- ■ POA&M for every gap, with dates and owners (POA&Ms allowed only for select 1-point items at L2 certification).
- ■ Policies mapped to all 14 control families — written to how you actually operate.
- ■ Evidence per control: screenshots, configs, exports, tickets — collected continuously, not the week before.
- ■ Vendor/subcontractor flow-down: who touches CUI downstream and their compliance status.
- ■ Security awareness training records for everyone in scope.

PHASE 4 — Assess & score (weeks 10–16)

- ■ Run the official DoD scoring methodology honestly (or use our free calculator below).
- ■ Submit your score to SPRS — required under DFARS 7019 before contract award.
- ■ For L2 certification: select a C3PAO early; lead times are real.
- ■ Fix the 5-point items first — they move your score 5× faster than 1-point items.

SPRS SCORING CHEAT SHEET

You start at **110** and subtract the weight of every control not fully implemented. Scores range from **+110 down to –203**.

Weight	Controls	What they are
–5 points	44 controls	Basic safeguarding failures — MFA, FIPS crypto, access control, CUI protection fundamentals
–3 points	14 controls	Significant weakening — audit, config management, maintenance controls
–1 point	51 controls	Limited exposure — procedural and supporting controls

- **Special partial credit — MFA (3.5.3):** MFA for remote & privileged users only = subtract 3 instead of 5.
- **Special partial credit — FIPS (3.13.11):** encryption in place but not FIPS-validated = subtract 3 instead of 5.
- **SSP (3.12.4):** no SSP = no valid assessment at all — this is the first document an assessor requests.
- **Temporary deficiencies:** only count as implemented when an enforced, documented plan exists.

Free tools (no signup): **itsecops.cloud/sprs-score-calculator/** — full 110-control calculator with official weights · **itsecops.cloud/cmmc-cost-roadmap-planner/** — cost & timeline planner · **itsecops.cloud/cmmc-cost-index/** — what CMMC really costs, 8 contractor profiles.

THE 14 CONTROL FAMILIES AT A GLANCE

3.1 Access Control (22)
Least privilege, remote access, session control

3.2 Awareness & Training (3)
Role-based security training, insider threat

3.3 Audit & Accountability (9)
Logging, review, protection of audit records

3.4 Configuration Mgmt (9)
Baselines, change control, least functionality

3.5 Identification & Auth (11)
MFA, password policy, replay resistance

3.6 Incident Response (3)
IR capability, reporting, testing

3.7 Maintenance (6)
Controlled maintenance, sanitized media

3.8 Media Protection (9)
CUI media marking, encryption, disposal

3.9 Personnel Security (2)
Screening, termination protections

3.10 Physical Protection (6)
Facility access, visitor control

3.11 Risk Assessment (3)
Risk + vulnerability scanning cadence

3.12 Security Assessment (4)
SSP, POA&M, periodic assessment

3.13 System & Comms (16)
Boundary defense, FIPS crypto, DNS filtering

3.14 System Integrity (7)
Malware defense, monitoring, patching