



Norman Quality Tools

CMMC Level 2 / NIST SP 800-171 Kit

SAMPLE PREVIEW

SSP template, 110-requirement self-assessment with SPRS calculator and POA&M, 14 policy families and an incident response plan — now with a worked example and a step-by-step implementation guide.

What's inside
01 System Security Plan — SSP template
02 SPRS Self-Assessment & POA&M — 110 requirements, score, POA&M, asset inventory
03 Policy Templates (14 families) — policy set
04 Incident Response Plan — IR plan and 72-hour reporting
Examples/ — filled-in worked example (fictional company)
Implementation Guide — order of steps, RACI, time estimates, 30/60/90 plan, audit-prep checklist, auditor findings, FAQ

Templates, not legal or regulatory advice. Not a CMMC assessment or certification.
Pages that follow are excerpts. Example pages show fictional data.

© 2026 Norman Quality Tools. All rights reserved.



CMMC Level 2 / NIST SP 800-171 Kit: Implementation Guide

Step-by-step rollout for a small shop (about 10–50 people). Read this guide first.

Doc no.	Rev	Date	Approved by
NQT-CMMC-00	A	2026-10	_____

Templates, not legal or regulatory advice. Not a CMMC assessment or certification. Clause and section numbers are cited for navigation only; this guide paraphrases and does not reproduce any standard. NIST SP 800-171 Rev 2 is a free download from csrc.nist.gov (U.S. government work); CMMC Level 2 uses Rev 2, even though NIST has since published Rev 3; confirm requirements against it, your contract (DFARS 252.204-7012) and customer flow-downs.

Status note: CMMC status (checked 21 Oct 2026): on 13 Jul 2026 DoD suspended CMMC Phase 2, including the 10 Nov 2026 start of Level 2 (C3PAO) assessment requirements. This is a DoD policy suspension; the CMMC rule (32 CFR 170) has not been amended. NIST SP 800-171 Rev 2 and DFARS 252.204-7012 still apply. Confirm current requirements in your contracts. Source: Under Secretary of War (A&S) memo 26-P-1023, 13 Jul 2026, implementing the DoW CIO's suspension of CMMC Phase 2; dodcio.defense.gov/CMMC/about.

Not affiliated with or endorsed by the U.S. Department of Defense, NIST, the Cyber AB, any C3PAO, or any employer of the author.

1. What is in this kit

File	Use it for
01 System Security Plan	SSP template
02 SPRS Self-Assessment & POA&M	110 requirements, score, POA&M, asset inventory
03 Policy Templates (14 families)	policy set
04 Incident Response Plan	IR plan and 72-hour reporting

2. Order of steps

Step	What to do	Kit file	Clause / ref.	Est. time (small shop)
1	Scope: find where CUI lives; fill the asset inventory and boundary	02 Asset Inventory; 01 §1–2	32 CFR 170 scoping	6–10 h
2	Self-assess all 110 requirements; record evidence	02 Assessment	NIST SP 800-171 Rev 2 §3.1–3.14	16–24 h
3	Calculate SPRS score; build POA&M for gaps	02 Dashboard, POA&M	DoD Assessment Methodology	3–4 h
4	Adopt and tailor the 14 policy families	03	§3.x families	10–16 h
5	Write the SSP describing how each requirement is met	01	3.12.4	16–24 h

6	Stand up incident response and 72-hour reporting	04	DFARS 252.204-7012(c)	4-6 h
7	Remediate POA&M items (MFA, FIPS encryption, logging, etc.)	02 POA&M	varies	20-60 h
8	Post score in SPRS; senior official affirms	02 Dashboard	32 CFR 170.22; DFARS 252.204-7019/7020	1-2 h
9	Annual affirmation (32 CFR 170.22); Level 2 self-assessment at least every 3 years (170.16)	all	32 CFR 170.22, 170.16	8-12 h/yr

Total effort: About 80-150 hours of staff time plus tool/IT costs over 3-6 months for a 10-50 person shop, depending on starting maturity.

3. Who owns what (RACI)

R = Responsible, A = Accountable, C = Consulted, I = Informed. Rename roles to fit your org chart; one person often wears several hats.

Activity	Senior Official	IT/Security Lead	Quality/Contracts	MSP (if any)	All staff
CUI scoping	A	R	C	C	I
Self-assessment	A	R	C	C	I
Policies	A	R	C	C	I
SSP	A	R	C	C	I
POA&M remediation	A	R	I	R	I
Incident reporting	A	R	C	C	C
SPRS posting & affirmation	A/R	C	C	I	I
Security awareness training	A	R	I	C	R

EXAMPL Plan of Action & Milestones (POA&M)

One row per Not Met / Partial requirement. Close within 180 days of a Conditional status.

CMMC Level 2 / NIST SP 800-171 Kit v1, Rev A (2026-10) | Norman Quality Tools | Template, not an assessment

[illegible]



4.2 Awareness and Training (AT)

ID	Requirement	Status	Implementation statement	Evidence
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder

4.3 Audit and Accountability (AU)

ID	Requirement	Status	Implementation statement	Evidence
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder
3.3.3	Review and update logged events.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder
3.3.4	Alert in the event of an audit logging process failure.	Not Met – POAM-001	Planned: SIEM alert on log-source failure (POAM-001, target 2026-11-30).	Screenshot / export dated 2026-03 in evidence folder
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Implemented	Implemented per policy (see 03 Policy Templates); configuration in IdP / Intune baseline.	Screenshot / export dated 2026-03 in evidence folder



EXAMPLE – FICTIONAL DATA — Example Precision Machining LLC is fictional. Names, part numbers and dates are invented to show how the form is completed.

Document control

Doc no.	Rev	Date	Approved by
EPM-CMMC-04	B	2026-03-02	Dana Whitfield, Quality Manager

Incident Response Plan & 72-Hour Reporting

CMMC Level 2 / NIST SP 800-171 Kit - Document 04 - Rev A (2026-10)

1. Incident response team

Role	Name	Phone	Backup
Incident lead	Marcy Chen	(555) 010-0000 (fictional)	Ken Albright
IT administrator	Marcy Chen	(555) 010-0000 (fictional)	Ken Albright
Senior official	Ken Albright	(555) 010-0000 (fictional)	Dana Whitfield
Outside IT / MSP	N/A – IT is in-house	—	—
Legal counsel	Jordan Reyes, outside counsel, Reyes & Hart LLP (fictional)	(555) 010-0000 (fictional)	Ken Albright

2. Phases

1. Prepare: keep contacts, logs and backups current; hold a medium assurance certificate for DIBNet reporting.
2. Detect and analyze: log the time of discovery. That starts the 72-hour clock.
3. Contain: isolate affected systems; do not wipe them (images must be preserved).
4. Report: if covered defense information or operationally critical support is affected, report at <https://dibnet.dod.mil> within 72 hours (DFARS 252.204-7012(c)); tell your prime/customer per contract.
5. Preserve: keep images of affected systems and relevant monitoring/packet data for at least 90 days from the report (DFARS 252.204-7012(e)); submit malicious software to DoD Cyber Crime Center if found (7012(d)).
6. Eradicate and recover; then lessons learned within 2 weeks; update SSP and POA&M.

3. Incident log

#	Discovered (date/time)	Reported by	Description	CUI involved?	DIBNet report # / time	Closed
IR-26-001	2026-05-04 09:40	Luis Ortega	Phishing link clicked on cad-02; mailbox held CUI drawings; no exfiltration found	Yes	Reported 2026-05-05 08:15 (within 72 h); report no. EX-0001 (fictional)	2026-05-06