WRIGHTBRAINED
SECURITY

FREE CHECKLIST · CMMC

What Assessors Ask to See

An evidence checklist for NIST SP 800-171 and CMMC Level 2, written from the assessor's side of the table. Policies say what you intend to do. Evidence shows that you did it.

How assessors decide "met"

Every one of the 110 requirements is broken into smaller assessment objectives, and every objective has to be supported. Assessors use three methods, and a policy only covers one of them.

EXAMINE
Documents, settings, logs, records and diagrams.

INTERVIEW
The people who run the control explain how it works.

TEST
Watching the control work live. A screenshot is not a test.

Rules that save you a redo

1. **Ask your assessment firm (C3PAO) how current evidence must be.** Ninety days is a sensible default, but ask first.
2. **Screenshots show the whole screen,** with the date and time, the system or tenant name, and the setting name and value. Never crop to hide or edit anything.
3. **Match the SSP.** If your System Security Plan says it, the evidence should show exactly that.
4. **Show every account or device, not one.** One user's MFA screen doesn't prove everyone has it.
5. **Name files by requirement,** for example `3.5.3_MFA-policy_2026-09-15.png`.

The checklist

Check each item off when you can put your hands on it in under five minutes. Anything that takes longer is a gap worth fixing now.

Access Control

AC · TALK TO: SYSTEM ADMIN, IDENTITY/IT LEAD, A REGULAR USER

- [ ] Current list of user accounts with role, and proof it was reviewed (who, when, what changed)
- [ ] Account request and approval records for a recent new hire, and the removal record for a recent leaver
- [ ] Group or role membership showing admins are few, named, and separate from everyday accounts
- [ ] Account lockout, session lock and logon banner settings, shown from the live system
- [ ] Remote access setup: VPN or gateway settings, encryption in use, and remote session logs
- [ ] Wireless settings (authentication and encryption) and the list of approved access points
- [ ] Mobile device management showing enrolled devices, encryption and who is allowed to connect
- [ ] List of outside systems you connect to (cloud, partners) and how each is approved
- [ ] Who approves anything posted to public websites, with an example of the review

Awareness and Training

AT · TALK TO: HR OR TRAINING OWNER, A FEW STAFF MEMBERS

- [ ] Training completion records by person and date for the most recent cycle
- [ ] Role-based training for admins and security staff (not just the annual video)
- [ ] Insider threat awareness content and who completed it

Audit and Accountability

AU · TALK TO: WHOEVER REVIEWS LOGS (IN-HOUSE OR YOUR SOC/MSSP)

- [ ] List of which events are logged, and when that list was last reviewed
- [ ] Log samples from key systems showing user, time, event and outcome
- [ ] Evidence someone actually reviews logs: tickets, review notes or SOC reports with dates
- [ ] Alert setup for logging failures, and an example alert
- [ ] Time sync settings pointing to an authoritative source
- [ ] Who can change or delete logs (it should be a very short list)

Configuration Management

CM · TALK TO: IT LEAD OR MSP, CHANGE APPROVER

- [ ] Hardware and software inventory that matches what is actually on the network
- [ ] Baseline configurations (for example Intune or group policy settings) and the date they were approved
- [ ] Change tickets showing request, security review, approval and completion for recent changes
- [ ] List of blocked or disabled programs, ports and services, with the reason each is allowed
- [ ] Application allowlisting or blocklisting policy and proof it is enforced
- [ ] How user-installed software is prevented or monitored

Identification and Authentication

IA · TALK TO: IDENTITY ADMIN, A REGULAR USER (FOR A LIVE MFA DEMO)

- [ ] MFA policy covering privileged accounts (local and network) and all users over the network
- [ ] A live MFA prompt for an admin account, and for a regular account
- [ ] Password settings: length and complexity, reuse limits, temporary password change
- [ ] Inactive account settings and a report of disabled accounts
- [ ] Service accounts and how they authenticate

Incident Response

IR · TALK TO: INCIDENT LEAD, LEADERSHIP CONTACT

- [ ] Incident response plan with roles, contacts and reporting steps (including DFARS 72-hour reporting)
- [ ] Incident or ticket log showing how incidents were tracked and closed
- [ ] Results of your most recent tabletop or test, with the follow-up actions

Maintenance

MA · TALK TO: IT LEAD OR MSP

- [ ] Maintenance records for key systems
- [ ] How remote maintenance sessions are approved, protected with MFA and ended
- [ ] Escort or supervision records for outside technicians
- [ ] How equipment is sanitized before it goes out for repair

Media Protection

MP · TALK TO: IT LEAD, OFFICE MANAGER

- [ ] Removable media policy and the technical control that enforces it
- [ ] Where CUI media is stored and who can get to it
- [ ] Sanitization or destruction records (certificates or a log)
- [ ] How backups containing CUI are protected and encrypted
- [ ] CUI marking examples

Personnel Security

PS · TALK TO: HR

- [ ] Screening records (background checks) before access is granted
- [ ] Offboarding checklist and a recent example showing access removed on time

Physical Protection

PE · TALK TO: FACILITIES OR OFFICE MANAGER

- [ ] List of people with physical access, and how it is reviewed
- [ ] Visitor logs and escort procedure
- [ ] Badge or key inventory, including lost or returned badges
- [ ] Cameras, alarms or other monitoring, and who watches them
- [ ] Home office or alternate site rules for CUI

Risk Assessment

RA · TALK TO: SECURITY LEAD

- [ ] Your most recent risk assessment and risk register
- [ ] Vulnerability scan reports from recent cycles
- [ ] Tickets showing scan findings were fixed within your stated timelines

Security Assessment

CA · TALK TO: SECURITY LEAD, LEADERSHIP

- [ ] System Security Plan (SSP) that matches the environment today, with owners named
- [ ] Your POA&M with owners, dates and progress
- [ ] Records of periodic control reviews and ongoing monitoring

System and Communications Protection

SC · TALK TO: NETWORK ADMIN OR MSP

- [ ] Network diagram and data-flow diagram showing where CUI lives and moves
- [ ] Firewall rules showing deny by default, and the reason for each allowed rule
- [ ] Proof of FIPS-validated encryption for CUI in transit and at rest (with certificate numbers)
- [ ] Split tunneling setting on the VPN
- [ ] Settings that block remote activation of cameras and microphones
- [ ] How encryption keys are managed

System and Information Integrity

SI · TALK TO: IT LEAD, SOC/MSSP

- [ ] Patch compliance report and your patching timelines
- [ ] Malware protection (EDR) deployment count compared to your inventory
- [ ] Proof malware definitions update automatically
- [ ] Monitoring and alerting setup, and a recent alert that was handled
- [ ] How you receive and act on security advisories