

Can You Prove It?

The 20-Point CMMC Evidence Readiness Checklist

How prepared is your organization to defend its cybersecurity self-assessment? Requirements may continue to evolve, but defense suppliers still need to understand how CUI is protected and demonstrate their cybersecurity practices. Use this checklist to identify potential gaps.

1. Score each statement

Give yourself 1 point for every statement you can confidently answer "Yes" — and support with evidence.

2. Add up your section scores

Each section is worth up to 5 points. Add your four section scores for a total out of 20 points.

3. Flag what you cannot prove

If a statement is true but you cannot identify what evidence would prove it, mark it "Needs Review" and skip the point.

A

Know Your CUI

Can you trace it?

- ☐ We know where CUI enters our organization.
- ☐ We know every system that stores CUI.
- ☐ We know which systems process CUI.
- ☐ We know how CUI is transmitted internally and externally.
- ☐ We know which users and third parties can access CUI.

SECTION SCORE **0** / 5

B

Control Your Scope

Can you contain it?

- ☐ We have a documented CUI/security boundary.
- ☐ CUI does not unnecessarily move into corporate systems.
- ☐ External sharing occurs through approved workflows.
- ☐ Access to CUI is limited to authorized users.
- ☐ Identity and authentication controls are documented and enforced.

SECTION SCORE **0** / 5



Document What You Do

Does the paperwork match reality?

- ☐ Our SSP reflects the way our environment actually operates today.
- ☐ Security requirements have defined owners.
- ☐ Our POA&Ms reflect current remediation activities.
- ☐ Policies and procedures match actual operational practices.
- ☐ Documentation is reviewed whenever significant systems or processes change.

SECTION SCORE **0** / 5



Prove It

Could you demonstrate it tomorrow?

- ☐ We have objective evidence supporting implemented security requirements.
- ☐ Evidence can be mapped to the appropriate requirement.
- ☐ Evidence is current and accessible.
- ☐ Our team can explain how controls operate — not simply produce a policy.
- ☐ We could assemble supporting evidence quickly if a customer or assessor asked.

SECTION SCORE **0** / 5

YOUR READINESS SCORE



0 / 5



0 / 5



0 / 5



0 / 5

TOTAL 0 / 20

This checklist is a readiness indicator — not a CMMC assessment, certification score or official assessment result.

17–20

POINTS

Strong evidence foundation

You appear to have the core elements of a defensible cybersecurity posture in place.

FOCUS NEXT ON

Keeping evidence current as your environment changes.

12–16

POINTS

Evidence gaps may exist

You may have many practices in place, but uneven scope or evidence makes them hard to defend.

FOCUS NEXT ON

Finding which “Yes” answers you cannot yet demonstrate.

0–11

POINTS

A structured readiness review may be warranted

Start with where CUI lives, how your environment is defined, and how requirements get documented.

FOCUS NEXT ON

Building the foundation before assembling evidence.

THE MOST IMPORTANT QUESTION

For every cybersecurity requirement where you answered "Yes," ask: "What would we show someone to prove it?"

If the answer isn't immediately apparent, change the answer to "Needs Review."

Exostar helps Defense Industrial Base organizations establish more controlled CUI collaboration environments, manage identity and access, assess cybersecurity requirements, organize documentation and evidence, and prepare for changing government requirements.

Protect.

Reduce.

Document.

Prove.

THE NEXT STEP

Request a CUI & CMMC Readiness Review

Talk to Exostar