PENTESTERRA

CMMC 2.0 LEVEL 2 GAP ASSESSMENT

Are Your Systems Ready for a DoD Contract?

Gap assessment across all 110 CMMC 2.0 Level 2 practices (equivalent to NIST SP 800-171 Rev.2) for US Department of Defense contractors handling CUI.

IN SHORT

Covers all 110 CMMC 2.0 Level 2 practices across 14 domains (AC, AT, AU, CM, IA, IR, MA, MP, PS, PE, RA, CA, SC, SI) - equivalent to the 110 practices in NIST SP 800-171 Rev.2.

110

CMMC 2.0 Level 2 practices covered

14

Domains: AC, AT, AU, CM, IA, IR, MA, MP, PS, PE, RA, CA, SC, SI

DoD

Subcontractors and suppliers handling CUI

THE SITUATION TODAY

WHO YOU ARE

You're the security lead of a US Department of Defense subcontractor that handles Controlled Unclassified Information (CUI) and needs CMMC 2.0 Level 2 certification.

WHAT HAPPENED

A DoD contract requires CMMC certification as a condition of bidding, and the 110 practices have never been systematically verified.

WHY IT HURTS

Without CMMC certification, a company loses eligibility to bid on US Department of Defense contracts and subcontracts - a direct commercial exclusion, not just a theoretical risk.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

Pentesterra's CMMC 2.0 Level 2 Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of CMMC 2.0 Level 2, grouped the way you'll see them in the platform.

Access Control and Identification (AC, IA)

The largest domain: who can access what and how they're authenticated.

- Limiting access to authorized users
- Multi-factor authentication
- Automatic session lock

Audit, Configuration, Incident Response (AU, CM, IR)

Traceability, configuration and incident handling.

- Audit logs and analysis capability
- Secure configuration baselines
- Incident response plan and team

Media, Personnel, Physical (MP, PS, PE)

Protection of media, people and physical environments.

- Marking and secure disposal of media
- Screening of personnel with CUI access
- Physical access control

Risk, Assessment, System/Comms, System Integrity (RA, CA, SC, SI)

Risk assessment and technical protection of systems.

- Periodic risk assessment
- Protection of network boundaries
- Protection from malicious code

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for CMMC 2.0 Level 2

A complete report, ready to present to clients, auditors, or your board.

Request your CMMC 2.0 Level 2 Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance