CONFIANCE CYBERSECURITY

CMMC Level 2 and Controlled Unclassified Information (CUI)
What you need to know

What Is CMMC?

The **Cybersecurity Maturity Model Certification (CMMC)** is a U.S. Department of Defense (DoD) cybersecurity standard for defense contractors and subcontractors. Its purpose is to ensure that organizations handling government information have adequate cybersecurity practices in place.

Unlike older self-attestation models, CMMC requires third-party certification by an accredited CMMC Third-Party Assessment Organization (C3PAO) or an authorized assessor.

Why CMMC Exists

DoD contractors often handle sensitive but unclassified government information known as **Controlled Unclassified Information (CUI)**. This can include:

- Contract proposals
- Technical drawings
- Specifications
- Test plans and test results
- Program management data

If this information is exposed or stolen, it can create national security risks, result in loss of competitive advantage, or jeopardize DoD programs. CMMC exists to verify that contractors have appropriate controls in place to protect CUI.

CMMC Model at a Glance

CMMC is structured into multiple maturity levels. Each level includes practices that build on the previous level.

Level	Purpose	When It Applies
1	Protect Federal Contract Information (FCI)	Lowest sensitivity contract data
2	Aligns with NIST SP 800-171	Handling of CUI
3	Enhanced protection	Higher-risk CUI environments

(Levels 4 and 5 exist but are not yet commonly required.)

CMMC Level 2 Overview

CMMC Level 2 is typically required for contractors that handle CUI.

Key characteristics include:

- Based on 110 security practices from NIST SP 800-171
- Requires documented policies and procedures
- Assessed by an independent assessor
- Certification is pass or fail, not self-attested

What Organizations Must Do

To achieve Level 2, an organization must:

1. Determine scope by identifying where CUI is stored, processed, or transmitted.
2. Document security controls through formal policies and procedures.
3. Implement technical, administrative, and operational controls.
4. Collect evidence showing controls are operating effectively.
5. Complete a formal assessment conducted by a C3PAO.

Confiance Cybersecurity
info@confiancecyber.com
confiancecyber.com
(970) 302-1194

Understanding CUI

Controlled Unclassified Information

CUI is government data that is not classified but still requires safeguarding due to its sensitivity. Examples include:

- Export-controlled technical data
- Program management information

Contract deliverables containing technical details

CUI is defined by federal regulations and marked according to DoD requirements when included in a contract.

Why CUI Matters for CMMC

You will likely fall under CMMC Level 2 if your organization:

- Receives CUI from a prime contractor
- Processes CUI on behalf of the DoD
- Store CUI in any system

If your organization never handles CUI, CMMC Level 1 may be sufficient. However, many prime contractors expect Level 2 readiness to ensure future eligibility.

How Scoping Works

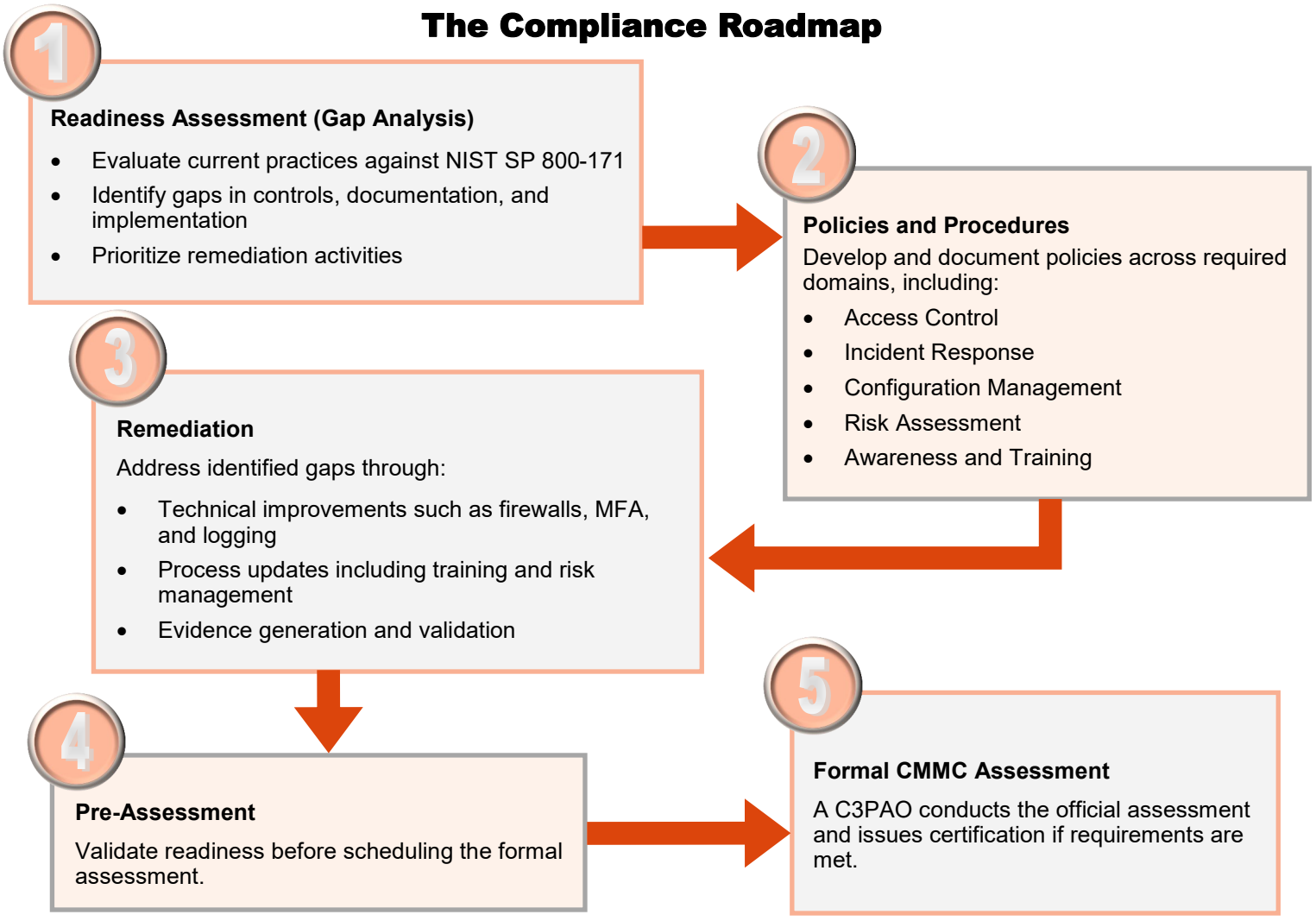
Scoping determines which systems, users, and processes fall under CMMC requirements. Important scoping questions include:

- **Where will CUI reside?**
- **Who will access CUI?**
- **Which systems store, process, or transmit CUI?**

What devices, services, or networks connect to those systems?

Some organizations use a CUI enclave, which is a dedicated and secured environment where CUI is handled. This approach limits compliance requirements to a smaller footprint and can significantly reduce complexity and cost.

The Compliance Roadmap



CONFIANCE CYBERSECURITY

Confiance Cybersecurity
info@confiancecyber.com
confiancecyber.com
(970) 302-1194

People and Security

CMMC Level 2 includes personnel security requirements such as:

- Background checks for individuals with CUI access
- Role-based access controls
- Ongoing security awareness training

Personnel security is a required component of compliance.

Costs to Consider

Costs vary based on organization size, scope, and technical maturity. Common cost categories include:

- Readiness assessment and consulting
- Policy and procedure development
- IT security improvements
- Background checks
- Third-party audit fees

Total costs depend heavily on scoping and remediation needs.

Are you Level 2?

- ☐ **You receive technical data from a prime contractor**
- ☐ **You store contract deliverables on internal systems**
- ☐ **You share drawings or specs via email or file portals**
- ☐ **Your contracts reference DFARS 252.204-7012 or CUI**

If you checked any of these, CMMC Level 2 likely applies.

Common Mistakes We See

- Assuming cyber insurance equals compliance
- Treating policies as paperwork instead of audit evidence
- Under-scoping systems and users
- Waiting until contract award to start preparation
- Relying on self-attestation assumptions
- Failing to maintain evidence over time

Confiance is here to help!

How We Help Organizations Prepare for CMMC Level 2

- CUI scoping and enclave design
- NIST 800-171 gap assessments
- Policy and procedure development
- Remediation planning and validation
- Pre-assessment readiness reviews

Get clarity before certification becomes mandatory.
Schedule a readiness discussion today.

CONFIANCE CYBERSECURITY

Confiance Cybersecurity
info@confiancecyber.com
confiancecyber.com
(970) 302-1194