CMMC Levels 1, 2 & 3 In a Brief

LEVEL 01

FOUNDATIONAL

Basic safeguarding of Federal Contract Information (FCI).

INFORMATION PROTECTED
FCI

REQUIREMENTS
15
requirements

FRAMEWORK
FAR 52.240-93
(formerly FAR 52.204-21)

ASSESSMENT
Annual self-assessment

ACCOUNTABILITY
Annual affirmation in SPRS

CISO FOCUS
Establish and verify baseline safeguards.

LEVEL 02

ADVANCED

Protection of Controlled Unclassified Information (CUI).

INFORMATION PROTECTED
CUI

REQUIREMENTS
110
requirements

FRAMEWORK
NIST SP 800-171
Revision 2

ASSESSMENT
Self-assessment or authorized third-party assessment, depending on contract requirements.

ACCOUNTABILITY
Annual affirmation; assessment cycle generally three years.

CISO FOCUS
Demonstrate control implementation, evidence and sustained compliance.

LEVEL 03

EXPERT

Enhanced protection against advanced threats for designated high-priority programs.

INFORMATION PROTECTED
CUI + enhanced protections

REQUIREMENTS
110 + 24
110 NIST SP 800-171 requirements plus 24 selected requirements from NIST SP 800-172

ASSESSMENT
Government-led assessment by DIBCAC

ASSESSMENT CYCLE
Generally three years
under the program model

ACCOUNTABILITY
Annual affirmation

CISO FOCUS
Address advanced persistent threats and validate enhanced safeguards.

WHAT CISOs SHOULD VERIFY FIRST

01 Information scope
Do your systems handle FCI, CUI or both?

02 Contract requirement
Which CMMC level and assessment type does the solicitation or contract specify?

03 System boundary
Which systems, users, suppliers and services are in scope?

04 Evidence readiness
Can you demonstrate that required controls are implemented and operating?

05 Leadership accountability
Are assessment results and annual affirmations accurate and current?

www.ampcuscyber.com | letsconnect@ampcuscyber.com