CMMC 2.0 Compliance at a Glance

A **mandatory framework** for DoD contractors to protect sensitive defense information through tiered cybersecurity requirements.

The 3 Levels of CMMC 2.0

Level 1: Foundational

Handles:
Federal Contract Information (FCI)

- **Security Requirements:** 17 basic cyber hygiene practices
- **Assessment Method:** Annual Self-Assessment

Level 2: Advanced

Handles:
Controlled Unclassified Information (CUI)

- **Security Requirements:** 110 practices from NIST SP 800-171
- **Assessment Method:** Self-Assessment or Triennial 3rd-Party Audit

Level 3: Expert

Handies:
CUI Critical to National Security

- **Security Requirements:** 110+ practices from NIST SP 800-172
- **Assessment Method:** Triennial Government-Led Audit

The High Stakes of Non-Compliance

Contract Cancellation

The DoD can terminate existing contracts, resulting in immediate loss of revenue.

Barred from Future Work

Non-compliance disqualifies your business from bidding on any new DoD contracts.

Significant Financial Penalties

Your business could face steep fines and fees for failing to meet security controls.

Damage to Reputation

Failing to comply can destroy trust with partners and cost you future opportunities.

The Computer Company