

thorough gap analyses are

Organizations completing

more likely to successfully implement key security controls required for CMMC 2.0 certification.

02

Documentation Maturity Drives

03

04

Stronger

Security

Fully documented cybersecurity policies directly correlate with significantly higher adherence to verified

encryption standards, with 83 compliance versus 49%

organizations.

among partially documented



Minimal Documentation Equals Major Security Risks

Organizations with

minimal cybersecurity

documentation are

more likely to inconsistently encrypt controlled unclassified information (CUI),

information (CUI), dramatically increasing their vulnerability.

Medium-sized organizations

(500-9,999 employees) have a

engagement

rate

with specialized external

and external expertise.

Engagement

Medium-sized

Firms Lead

in Partner

compliance partners, demonstrating

optimal balance of internal capabilities



\$

67 % 12-24 months

06

Advanced

Controls

Documentation

and Third-party

**Drives Encryption** 

41 % 6-12 months

policies maintain advanced third-party access controls, significantly strengthening their overall security posture.

of organizations with fully

documented cybersecurity

Executive
Perception
Gaps Highlight
Risks

CEOs and founders rate their cybersecurity documentation maturity significantly higher (80%) compared to cybersecurity leaders (54%), revealing critical gaps in internal communication and assessment accuracy.





