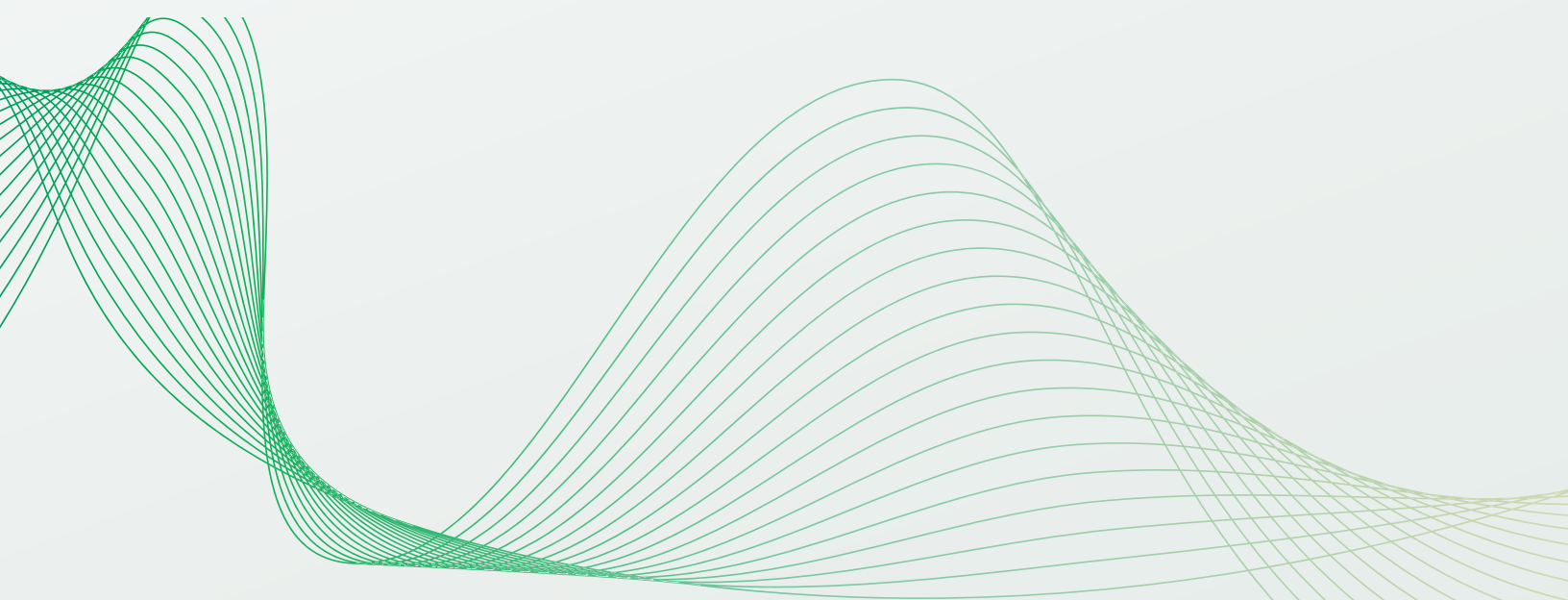


 READINESS CHECKLIST FOR 2026

CMMC 2.0

Readiness Checklist for 2026

How Government Contractors Can Secure Google
Workspace for Compliance with Qanapi



FEDRAMP
READY



NIST
800-171



HIPAA, CJIS, PCI DSS, ITAR, DFARS, FIPS
140-3 COMPLIANT

Government Contractors Face a Reality Check in 2026

Enforcement of Cybersecurity Maturity Model Certification (CMMC) has already begun, but research suggests most organizations are not prepared. The average defense contractor has a Supplier Performance Risk System (SPRS) score of **-12**—and just **4%** of organizations believe they're fully prepared for certification. This could start hitting companies' bottom lines in the new year.

Beginning in November 2026, many DoD contracts that involve CUI will require CMMC Level 2 certification from a third-party assessor as a condition of award. Rather than submitting self-assessments, vendors will have to pass third-party audits, meaning those that are unprepared will lose significant revenue.

Use this checklist to ensure your Google Workspace is compliance-ready—and your organization can win contracts in 2026 and beyond.

THE STATE OF CONTRACTOR CYBERSECURITY

56%

Lack full end-to-end encryption for sensitive data

79%

Don't require multi-factor authentication

36%

Cite budget constraints as their biggest barrier to CMMC compliance

What is CMMC 2.0?

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is the Department of War's framework for unifying and enforcing the patchwork of federal cybersecurity standards applicable to defense contractors.

In practice, this means that contractors handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) must now demonstrate—through independent assessment—that their systems meet the same NIST-based security controls already required of federal agencies.

This presents a series of challenges for CISOs, CIOs, compliance officers, and IT security teams.

3 Key Challenges for CMMC Compliance

1 | Technical Complexity

Roughly 31% of contractors say technical complexity is their biggest obstacle to CMMC compliance.

Many organizations lack the internal expertise required to design end-to-end architecture. From access controls to encryption, security leaders must manage multiple complicated integrations and ever-expanding vendor networks. This creates integration risk and could potentially delay procurement or deployment across departments—leading to lost productivity and even missed contracts.

2 | Audit Gaps

Contractors routinely overestimate their CMMC compliance posture.

Research has shown a discrepancy between internal audits and third-party verified tests—with organizations heavily overestimating their own preparedness. Many organizations struggle to map existing Zero Trust controls to CMMC requirements, leaving them with potentially costly compliance gaps.

3 | Dispersed Digital Workforces

The world of work has transformed over the last five years.

Digital collaboration across multiple devices—desktop, tablet, and mobile—is part of many teams' daily workflow. But this presents an extra level of difficulty to CMMC compliance, as most cybersecurity solutions are not built to work on all device types, potentially forcing security leaders to build workarounds or disrupt workflows.

THE CHECKLIST

Google Workspace CMMC Compliance Checklist

REQUIREMENT	NEED TO DO	DONE
Stay within a FedRAMP High / DoD IL4 compliant boundary	☐	☐
Enforce U.S.-only data residency	☐	☐
Restrict access to U.S. persons	☐	☐
Deploy strong identity and access controls	☐	☐
Enable encryption that meets NIST 800-171	☐	☐
Implement Data Loss Prevention (DLP)	☐	☐
Turn on full audit logging	☐	☐
Set retention and incident-response readiness	☐	☐
Review the Customer Responsibility Matrix (CRM)	☐	☐



Prepare for CMMC 2.0 with Qanapi

Qanapi Flow is the only solution engineered specifically for CMMC alignment. From access controls to live redaction for Google Docs and Slides, it delivers instant Zero Trust data security and privacy to help contractors pass compliance audits with confidence:

- ⚡ Installation takes less than 5 minutes, with no technical setup required
- 📱 Works across desktop, tablet, and mobile without integrations
- 🛡️ Backed by federal certifications and secure supply-chain standards.



Want to make CMMC compliance fast, simple, and cost-effective?

Sign Up Today →

SOURCES

1. <https://cybersheath.com/resources/downloads/defense-on-the-brink-the-perilous-state-of-cybersecurity-across-the-dib/>
2. <https://www.defenseandmunitions.com/news/kiteworks-warns-defense-contractors-of-multi-million-dollar-risks-if-cmmc-compliance-not-achieved/>
3. <https://cybersheath.com/resources/downloads/defense-on-the-brink-the-perilous-state-of-cybersecurity-across-the-dib/>
4. <https://www.kiteworks.com/report-cmmc-preparedness-dib/>
5. <https://www.kiteworks.com/report-cmmc-preparedness-dib/>
6. <https://cybersheath.com/resources/downloads/defense-on-the-brink-the-perilous-state-of-cybersecurity-across-the-dib/>