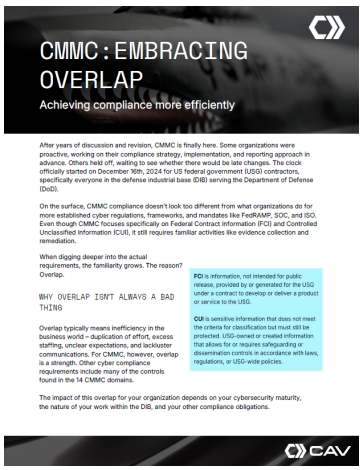

CMMC: Embracing Overlap

Achieving Compliance More Efficiently

Thank you for downloading this Cav resource. Carahsoft is the distributor for Cav cybersecurity solutions.

To learn how to take the next step toward acquiring Cav's solutions, please check out the following resources and information.

For additional resources:
carah.io/CaveonixResources

For upcoming events:
carah.io/CaveonixEvents

For additional Caveonix solutions:
carah.io/CaveonixProducts

For additional cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Caveonix@carahsoft.com
844-445-5688

CMMC: EMBRACING OVERLAP

Achieving compliance more efficiently

After years of discussion and revision, CMMC is finally here. Some organizations were proactive, working on their compliance strategy, implementation, and reporting approach in advance. Others held off, waiting to see whether there would be late changes. The clock officially started on December 16th, 2024 for US federal government (USG) contractors, specifically everyone in the defense industrial base (DIB) serving the Department of Defense (DoD).

On the surface, CMMC compliance doesn't look too different from what organizations do for more established cyber regulations, frameworks, and mandates like FedRAMP, SOC, and ISO. Even though CMMC focuses specifically on Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), it still requires familiar activities like evidence collection and remediation.

When digging deeper into the actual requirements, the familiarity grows. The reason? Overlap.

WHY OVERLAP ISN'T ALWAYS A BAD THING

Overlap typically means inefficiency in the business world – duplication of effort, excess staffing, unclear expectations, and lackluster communications. For CMMC, however, overlap is a strength. Other cyber compliance requirements include many of the controls found in the 14 CMMC domains.

FCI is information, not intended for public release, provided by or generated for the USG under a contract to develop or deliver a product or service to the USG.

CUI is sensitive information that does not meet the criteria for classification but must still be protected. USG-owned or created information that allows for or requires safeguarding or dissemination controls in accordance with laws, regulations, or USG-wide policies.

The impact of this overlap for your organization depends on your cybersecurity maturity, the nature of your work within the DIB, and your other compliance obligations.

CMMC DOMAINS

Many organizations will require CMMC Level 1, which focuses on the protection of FCI and features 15 requirements identified in 48 CFR 52.204-21 across the access control, identification and authentication, media protection, physical protection, system and communications protection, and system and information integrity domains.

As contracts grow in complexity and value, so do the expectations of the DoD. CMMC Levels 2 and 3 introduce requirements from NIST SP 800-171 and SP 800-172 across all 14 domains to cover the protection of CUI in addition to FCI.

There are 110 requirements for Level 2 and 134 for Level 3. When looking at the total, we see meaningful overlap between CMMC and several other common cyber compliance standards that can reduce the level of effort needed to achieve CMMC compliance.

% CMMC OVERLAP WITH OTHER FRAMEWORKS

FedRAMP 44%

AICPA SOC 41%

ISO 27001 67%

NIST 800-171 82%

Adding a new framework like CMMC to legacy compliance and GRC technologies often requires significant manual effort, effectively negating the benefits that could be realized through overlap between the new mandate and existing compliance efforts.

AUTOMATION UNLOCKS OVERLAP

The Cav compliance automation platform resolves this issue thanks to AI capabilities which associate controls and their accompanying evidence to the appropriate compliance

requirements. Organizations can add a new framework with just a few clicks, and it populates with all the information overlapping with existing frameworks so you get a comprehensive view of your CMMC compliance posture quickly.

Of course, achieving CMMC compliance requires more than designing and implementing effective controls. You also need to prove it through evidence and remediation. Many security, compliance, and audit teams feel the pain of evidence collection – manual spreadsheets, point-in-time screenshots, and dependence on other parts of the organization to deliver. With so much inefficiency, expert resources are diverted away from defensive priorities and get stretched too thin.

CAV WITHIN THE CYBER TECH ECOSYSTEM

To address this challenge, Cav continuously acquires compliance evidence from the cybersecurity technology stack. The evidence is then automatically associated with the relevant controls and the CMMC requirements along with any other impacted compliance obligations. The platform also has a built-in plan of action and milestones (POA&M) management system covering the entire lifecycle in conjunction with your existing ticketing system so you can easily capture open items, prioritize, and track progress.

CONCLUSION

CMMC presents another compliance challenge for the DIB, but with overlapping requirements and automated evidence collection, organizations have the opportunity to continuously comply with CMMC without experiencing continuous pain.

ABOUT CAV

Cav delivers continuous cyber assurance for mission-critical organizations by automating evidence collection, validating controls in real time, and eliminating the burden of manual compliance work. Powered by agentic AI, our Compliance OS monitors against 50+ frameworks, accelerates audits, and ensures you're always secure, always compliant, and always mission-ready.