secureframe

The Pocket Guide to CMMC 2.0

Part I: Understanding CMMC compliance

Implementing CMMC compliance requirements can help organizations protect information related to national security, prevent cyber attacks, win lucrative federal contracts, and more.

To reap these benefits, you must understand the fundamentals of CMMC compliance.

What is CMMC 2.0?

The Cybersecurity Maturity Model Certification (CMMC) is an assessment framework and assessor certification program based on NIST 800-171 with the addition of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.700 series clauses.

This framework was created by the U.S. Department of Defense to make sure that companies working with the DoD have strong cybersecurity practices to protect sensitive information.

Originally introduced in early 2020, an updated version — CMMC 2.0 — was released in November 2021. CMMC 2.0 introduced significant changes to simplify the certification process, align more closely with existing cybersecurity standards, and reduce the compliance burden on small businesses. These changes make the framework more practical and accessible while maintaining robust cybersecurity practices to protect sensitive information.

Key changes include:

- **Condensed five levels to three**: CMMC 2.0 streamlines the original model from five to three levels. Each level has progressively stringent cybersecurity practices and assessment requirements based on the type and sensitivity of the information the organization processes.
- **Aligned with NIST cybersecurity standards**: The CMMC 2.0 framework heavily aligns with NIST standards, particularly NIST SP 800-171 for Level 2 and both NIST SP 800-171 and NIST SP 800-172 for Level 3.

- **Streamlined assessments**: CMMC 2.0 aims to streamline and reduce the costs associated with the assessment process, allowing all companies at Level 1 and a subset of companies at Level 2 to demonstrate compliance through self-assessments.
- **Increased flexibility**: CMMC 2.0 also increases the flexibility of implementing requirements. Most notably, under certain limited circumstances, it allows companies to make Plans of Action & Milestones (POA&Ms) to achieve certification and allows the government to waive inclusion of CMMC requirements.

Is CMMC compliance mandatory?

All contractors and subcontractors that work with the DoD and handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) are required to have CMMC certification.

Why is CMMC compliance important?

As with other federal frameworks, CMMC compliance is important for two major reasons.

One is government contracting. CMMC certification is a requirement for organizations wishing to bid on and participate in DoD contracts. Without CMMC certification, companies cannot compete for DoD contracts that involve sensitive information.

The second is data security. Strong security and compliance measures can deter cyber criminals from attacking your organization and help keep your, your customers', your partners', and the American people's data safe. This will have important ramifications for the public sector, the private sector, and ultimately national security and privacy.

Part II: CMMC compliance requirements

CMMC is a derivative of NIST 800-171 that's specific to DoD contractors and any other organizations providing services involving CUI or FCI to government agencies.

CMMC 2.0 encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) clause 52.204.21 and the security requirements for CUI specified in NIST 800-171 per DFARS clause 252.204.7012. This clause specifies additional requirements beyond the NIST 800-171 security requirements, such as incident reporting and flowdown of requirements to subcontractors.

CMMC levels

CMMC 2.0 streamlines requirements to three levels of cybersecurity (Level 1, Level 2, Level 3). Each level has corresponding domains, which map directly to the NIST control families and NIST 800-171 framework.

Here is a high-level overview of the CMMC 2.0 model:

- **Level 1**: Foundational ensures that companies implement basic cybersecurity practices to protect FCI.
- **Level 2**: Advanced aligns with NIST SP 800-171 Rev 2 and is designed for organizations handling CUI.
- **Level 3**: Expert incorporates additional NIST SP 800-172 controls to protect against Advanced Persistent Threats (APTs). APTs are highly sophisticated and targeted cyberattacks designed to infiltrate a network, remain undetected for extended periods, and systematically extract valuable data.

The CMMC level that applies to an organization depends on the nature of the data it handles. Level 1 pertains to FCI. Levels 2 and 3 pertain to CUI.

An organization's CMMC level will also determine their eligibility to bid on a government contract or subcontract.

CMMC assessments

With DFARS clause 252.204.7012, DoD contractors could self-assess to NIST 800-171 compliance. When DFARS clauses 252.204.7019, 20, and 21 were released in 2020, they enforced CMMC assessments and required DoD contractors to do a NIST 800-171 assessment every three years and submit it to the DoD for review if bidding on 7012 contracts.

Below are the assessment requirements for each CMMC level:

- All L1 contractors and a subset of L2 contractors must complete and submit self-assessments annually.
- A subset of L2 contractors must undergo assessments by third-party organizations (C3PAO assessments) every three years. These assessments will be conducted against the NIST 800-171 standard.
- L3 contractors must complete government-led assessments every three years. These will be based on a subset of NIST 800-171 requirements.

Part III: Automating CMMC compliance

Compliance automation is a key disruptor in the government and public sector. With Secureframe's automated platform for example, government contractors and authorized software vendors can navigate complex requirements and achieve strong compliance outcomes for CMMC 2.0 as well as other federal frameworks.

Below, we'll explain how compliance automation software simplifies and streamlines the federal compliance process.

CMMC compliance with vs without automation

Manually getting compliant with CMMC and other federal frameworks is time-consuming, resource-intensive, and stressful.

You'll need to complete a thorough risk assessment and gap analysis, then design controls and write policies from scratch. You'll also need to train your staff on security best practices and make sure they all review the new policies. You'll have to update spreadsheets and grab hundreds of screenshots to use as evidence during your assessment. And you'll have to stay current on the latest requirements.

This will require dedicating multiple team members and company leaders to overseeing compliance, and likely hiring a consultant to assist you. Compliance automation software can eliminate some of this manual work, saving hundreds of hours and thousands of dollars on preparation and consultant fees.

Below are some of the most powerful benefits of Secureframe's automation platform and in-house expertise.

Federal compliance expertise

Secureframe's dedicated, world-class support team of former CMMC, FISMA, and FedRAMP auditors and consultants are there with you every step of the way to guide and consult you through federal readiness and audits and keep you up-to-date on the latest changes to federal compliance requirements.

Integrations to federal clouds

Secureframe integrates with your existing tech stack, including government cloud variants like AWS GovCloud, to automatically collect evidence.

Prebuilt and custom policies and templates

Templated policies, procedures, and SSPs written by former federal auditors are provided and can be fully customized to meet your needs. Secureframe's policy manager also supports the maintenance of policies in accordance with federal requirements.

Other templates, including a Separations of Duties Matrix, Plan of Action & Milestones (POA&M) documents, Impact Assessments, and readiness checklists, are provided as well.

In-platform training

With Secureframe, you can deliver in-platform, proprietary employee training that meets federal requirements including insider threat, information spillage, anti-counterfeit training, and role-based training such as secure coding. This is reviewed and updated annually by Secureframe compliance experts to ensure it continuously meets federal training requirements.

Role-based access controls

Security officers maintain control over the data that their users have access to on a role and need-to-know basis.

Custom controls and tests

Support for organizationally-defined and unique implementations for CMMC and all other frameworks is available.

Trusted partner network

Secureframe has relationships with auditors in partner networks that are certified Third Party Assessment Organizations (3PAOs) and CMMC 3PAOs (C3PAOs) that can support CMMC, FISMA, FedRAMP, and other federal audits.

Cross-mapping across frameworks

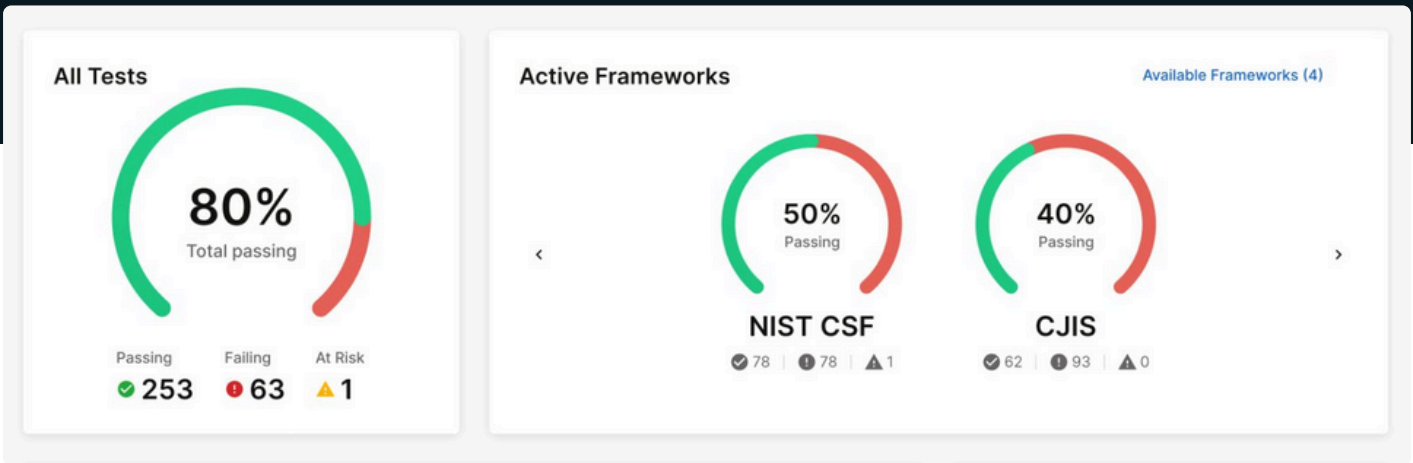
CMMC has a lot of overlapping requirements with NIST 800-53, FedRAMP, CJIS, and other federal frameworks. Instead of starting from ground zero, Secureframe's automation platform can help map what you've already done for one framework to other frameworks. That'll make it faster and easier to achieve compliance with additional standards and avoid duplicate efforts.

Continuous monitoring

By monitoring your tech stack 24/7 to alert you of non-conformities, Secureframe makes it easier to maintain continuous compliance. You can specify test intervals and notifications for required regular tasks to maintain compliance. You can also use Seucreframe's Risk Register and vulnerability scanning to support your continuous monitoring efforts and POA&M maintenance.

Federal Compliance with Secureframe

Secureframe is the automated compliance platform built by compliance experts to enable government contractors to navigate complex requirements. We cover CMMC 2.0, NIST 800-53, NIST 800-171, NIST CSF, NIST Privacy Framework, and CJIS.



secureframe

secureframe

Build trust. Unlock growth.

The leading, all-in-one automated security and privacy compliance platform

AUTOMATED EVIDENCE COLLECTION
Our 300+ integrations help you gather information from your existing tech stack automatically.

PREBUILT POLICIES
We provide standard templates for policies, procedures, and system security plans written by former federal auditors that can be edited to meet your specific needs.

ROLE-BASED ACCESS CONTROL
Security officers maintain control over the data that users have access to using role-based settings.

REPORTS AND DASHBOARDS
Get a clear view into your security posture and status, and see how you're progressing towards compliance.

AUTOMATED TESTS
View, assign, filter and export tests on a single page, and easily access all active and inactive tests from the Test Library.

CLOUD REMEDIATION WITH COMPLY AI
Secureframe helps fix failing cloud tests with step-by-step guidance and generative AI to provide infrastructure-as-code fixes.

IN-PLATFORM TRAINING
Secureframe delivers proprietary employee training for frameworks and in-platform tracking to help you stay compliant.

ACCESS TO COMPLIANCE EXPERTS
30+ dedicated compliance experts and former auditors help guide you through the process and recertifications.

TAILORED AUDITOR EXPERIENCE
We make it easy for auditors to review evidence and get through an audit quickly.

TAILOR YOUR COMPLIANCE PROGRAM
Create custom frameworks, controls, and tests that best fit your unique business needs.

TRUST CENTER
Showcase your security posture and remove friction from the end-to-end security review process.

QUESTIONNAIRE AUTOMATION
Save hundreds of hours answering RFPs and security questionnaires with Secureframe's ML-powered Questionnaire Automation.

TRUSTED BY TODAY'S LEADING COMPANIES

ramp · Teamable · Rand McNally · Magellan Jets · smartcar · Doodle · stream · wellfound: formerly AngelList Talent · lyra · GENERALI · The Salvation Army · Security Scorecard

> "Secureframe is a very user-friendly platform and has a great UI/UX. I can confidently say that the platform is so easy and it has everything you need to make getting SOC 2 [compliance] fast."
>
> **Thomas Mirmotahari**
> CEO and Co-Founder, PerkUp

Ready to automate your compliance?

Reach out to sales@secureframe.com or visit secureframe.com to learn more.