

Get Ready for CMMC Today

And Achieve Continuous Compliance for the Future

The Cybersecurity Maturity Model Certification (CMMC) framework consists of cybersecurity best practices and maturity processes.

What is a CMMC Framework?

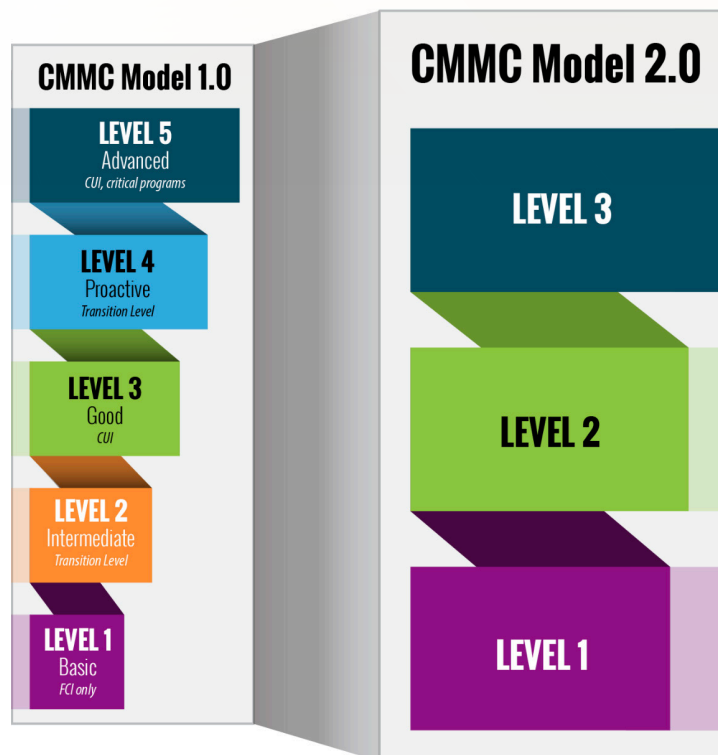
This framework is intended to protect federal contract information (FCI) and controlled unclassified information (CUI) with a goal of increasing assurance that federal contractors, and subcontractors within the supply chain, can adequately protect this information.

The Evolution of CMMC

The steady march forward of CMMC—despite some grumblings and internal reviews – signals big changes for organizations doing business with the Department of Defense (DoD).

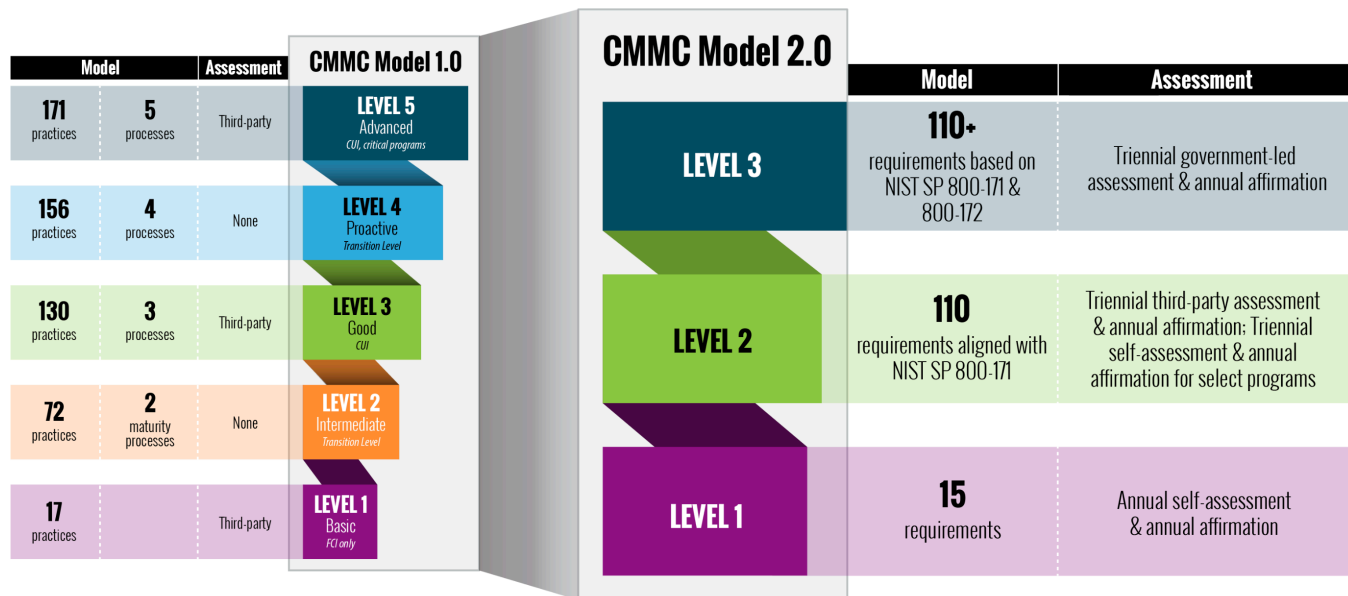
A key element in CMMC is the move away from the self-attestation model of prior efforts to a higher level of certification of contractors and subcontractors through a third party. Certification can be sought and achieved at one of three levels, ranging from basic hygiene (like anti-virus software) at Level 1 to the ability to detect and respond to advanced persistent threats (APTs) at Level 3.

Note: When comparing CMMC 1.0 to CMMC 2.0, you'll note the biggest change is a reduction from 5 levels in CMMC 1.0 to 3 levels in CMMC 2.0. To the right is an overview to illustrate this change.



Source: <https://dodcio.defense.gov/CMMC/Model/>

And a more detailed look at the particulars of each level, including the type of assessment per level :



Source : <https://dodcio.defense.gov/CMMC/about/>

Requirements at these levels will be familiar to many organizations. For example, CMMC 2.0 Level 2, includes the requirements specified in National Institute of Standards and Technology (NIST) SP 800-171 and other NIST publications. CMMC certification verifies the implementation of processes and practices at a particular level.

The Three Levels of a CMMC 2.0 Framework

As with most large-scale frameworks, ongoing internal review may slow some implementation efforts, but there's little doubt change is coming that will impact all DoD suppliers looking to get contract awards.

CMMC 2.0 is currently within the rulemaking process, and the DoD has indicated they do not intend to approve inclusion of a CMMC requirement in any contract prior to completion of the rulemaking process. So, while CMMC 2.0 is not a contractual requirement now, it will be. [Estimates from the DoD currently point to a 2024 implementation.](#)

At the conclusion of rulemaking, all DoD contracts are likely to contain CMMC requirements, and there is a possibility that other agencies will also adopt CMMC. Prime contractors must be worried about both their own certification and those of their subcontractors. Subcontractors might be facing third-party certification requirements for the first time. Satisfying CMMC requirements along with the growing demand to move workloads to the cloud presents critical challenges for the defense industrial base to overcome.

The Challenges with Ensuring and Maintaining Cloud Compliance

Cloud infrastructure and resource compliance is complex. Whether you are required to follow established guidelines such as FedRAMP or HIPAA or define your own standards, the sheer number of policies and resources in the cloud makes manual tracking a logistical nightmare. NIST SP 800-171 alone—a standard that makes up much of CMMC Levels 2 and 3—includes 110 policies, and each policy can apply to multiple resources. According to one study, 77% of IT decision makers believe that [they would not pass](#) all their cloud compliance audits for cloud resources.

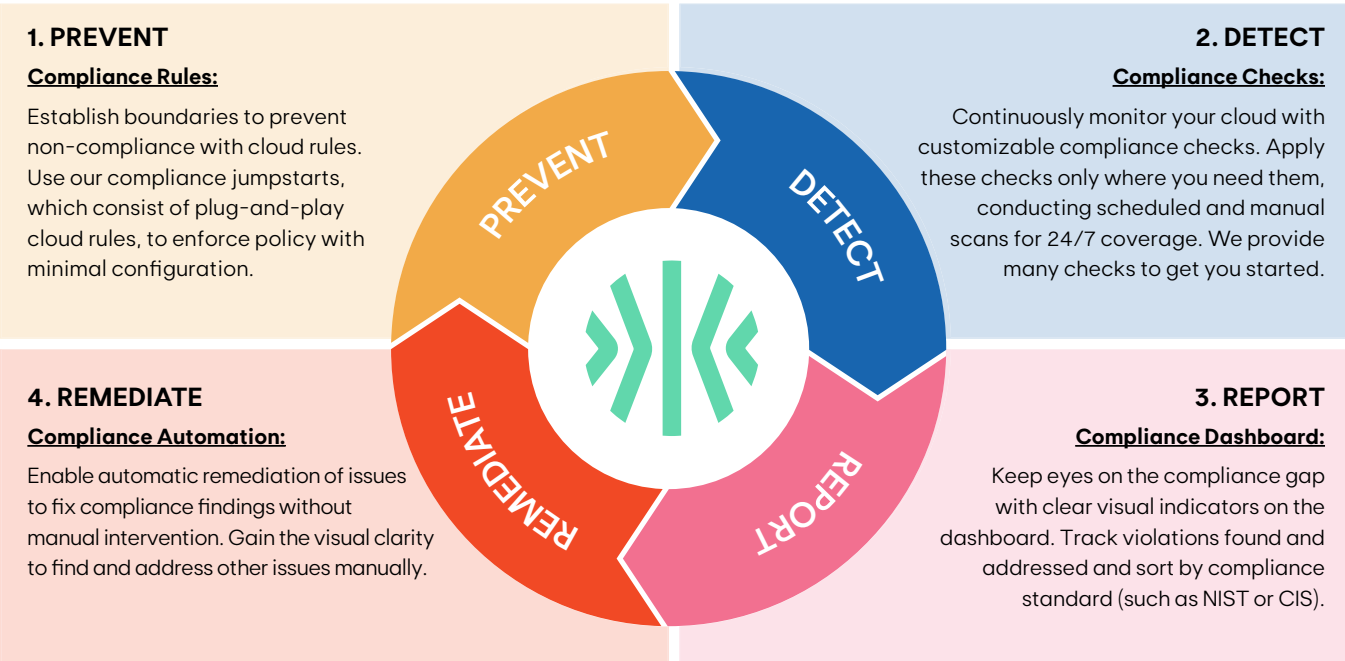
With the dynamic nature of the cloud, [achieving compliance](#) at one moment in time doesn't ensure compliance going forward. You could spend hundreds of hours tracking compliance manually. If you don't, you risk non-compliance, which leaves you exposed to potential security breaches or even civil or criminal penalties if you violate guidelines required by law. CMMC 2.0 requirements add the potential inability to compete for contract awards as a ramification of failed audits.

Kion helps you overcome these cloud compliance difficulties.

How Kion Eases the Path to Your CMMC 2.0 Framework Compliance

Kion is the only comprehensive solution that lets you manage and control your cloud infrastructure at scale. Kion automates end-to-end cloud provisioning— from account creation to sunseting—while enforcing access control and financial and compliance policies in the cloud.

Kion provides four key capabilities to [deliver continuous compliance](#).



To Support CMMC V2.0, Our Jumpstart Includes:

- ✓ 128 AWS compliance checks
- ✓ 249 Azure managed resources
- ✓ 12 AWS CloudFormation templates
- ✓ 9 AWS IAM policies
- ✓ 9 Azure ARM templates
- ✓ 10 Azure managed policy definitions
- ✓ 3 Azure role definitions
- ✓ 1 compliance standard containing all checks
- ✓ 1 yaml file to help you automate and expedite the creation of your System Security Plan (SSP)
- ✓ 4 Cloud Rules to decide if you want to simply report or also prevent CMMC 2.0 compliance violations and handle Incident Response actions across AWS and Azure
- ✓ 1 CMMC Control Matrix with complete control documentation, example responses, framework coverage metrics, and cross-references to other compliance frameworks that you'll need to satisfy the CMMC requirements

Using Kion to Achieve CMMC 2.0 Compliance is as Easy as 1, 2, 3

1. Assess Your Current Maturity Level

First, you must determine where you fall on the CMMC [three-level maturity rating](#). Many of the CMMC 2.0 requirements closely align with those from NIST SP 800-171. This standard offers cybersecurity guidance on issues such as multifactor authentication and cyber-incident response. Given this close alignment, assessing where you're at against the NIST SP 800-171 requirements can provide a good idea of whether security gaps exist and the prevalence of any gaps.

2. Use the Kion Platform to Jumpstart CMMC 2.0

Kion's 360-degree approach to compliance delivers both enforcement and audit capabilities in the form of jumpstarts. These jumpstarts help you expedite the path to CMMC 2.0 – and ensure ongoing security and compliance. Kion provides jumpstarts for CMMC, NIST SP 800-171, and NIST SP 800-53 (Rev. 4).

Jumpstart resources are compiled into Kion Cloud Rules that allow you to quickly start applying permissions and deploying resources into your managed accounts to rapidly achieve compliance. Cloud Rules include resources such as AWS IAM policies, CloudFormation templates, Microsoft Azure managed policies, Microsoft Azure Resource Manager templates, and Google Cloud IAM roles. These Cloud Rules can be customized directly within the Kion platform to give you the flexibility needed for your unique security posture and policy requirements.

Coverage is included for Levels 1 and 2 of CMMC 2.0. Kion provides 84% addressable coverage of required controls across Levels 1 and 2 for AWS; and 74% addressable coverage of required controls across Levels 1 and 2 for Azure.

3. Customize Jumpstarts to Meet Your Needs

Jumpstart assets are customizable, which is key because your environment and requirements are unique. For example, you can quickly and efficiently customize our tag enforcement scan for assets that match the prescribed tagging scheme for your organization. Jumpstarts do most of the policy writing for you, giving you the ability to customize to meet your needs.

The Value of Kion Compliance For Your CMMC 2.0 Framework

We built Kion compliance features from a base of deep expertise. Our team members have been through NIST hardening efforts and compliance audits at federal and intelligence community agencies. We've been responsible for ongoing security monitoring within organizations. We use that expertise to help you meet your compliance needs.

The Kion CMMC 2.0 jumpstart helps you satisfy framework requirements so you're business-ready to lead and support the capture of new contracts. However, preparing you for CMMC readiness is just the beginning of the value Kion brings to your organization.

Get Built-in Automation

There's a limit to the number of people you can assign to compliance efforts and there's a real risk of human error. Teams often manually apply security configurations on images or environments and then rely on regular scanning to verify infrastructure is still in a good state. These scans result in output that is usually not accessible by those who need to then address results, so the security engineer produces spreadsheets that then must be sent to each business owner. Kion supports the growing movement toward 'Compliance as Code' automation to help you tackle challenges like compliance visibility and manual effort. With Kion as the central hub, a security engineer can run scans using Kion compliance checks and automatically deliver results to business owners directly on Kion projects.

Reduce Compliance Implementation Time

Kion bundles compliance assets into Cloud Rules, which provide a targeted approach to compliance enforcement. Target one part of your business to apply a specific compliance regime, or apply a global regime at the top level and use inheritance to cascade down the controls. Our CMMC 2.0 jumpstart even includes assets to help you accelerate the production of your System Security Plan (SSP) by covering up to 60% of required efforts.

Streamline Audit Process and Prevent Panic

Security audit preparation and artifact creation take time and cause apprehension. For many organizations, the typical practice is to put in effort right before the audit, rather than continually monitoring and managing resources. As a result, you drift in and out of compliance and panic as you confront the work needed prior to an inspection. Kion's jumpstarts ease continuous compliance monitoring and include a Control Matrix, a re-listing of the compliance program controls that:

- Indicates the assets the Kion jumpstart provides for each control
- Identifies where the cloud service provider provides any coverage inherently
- Identifies where Kion provides any coverage inherently
- Provides control response verbiage to be used in an audit
- Includes recommendations on how to approach further covering a control

Our Control Matrix is your fast track for passing an audit, an artifact to indicate due diligence, and a workbook as you go through the process of prepping your environments.

Family	Title	Control	Severity	Description	Jumpstart Resources		
						Jumpstart Assets	Kion Platform
Authorized Access Control	AC.L1-3.1.1	AC.L1-3.1.1	Level 1	AC.1.001 AC.L1-3.1.1 Authorized Access Control Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). <ul style="list-style-type: none"> FAR Clause 52.204-21 b.1.i NIST SP 800-171 Rev 2 3.1.1 	AWS AWS Cloudformation Templates: <ul style="list-style-type: none"> - CMMC2-OrgWideCloudTrail - CMMC2-EventAuditingCentralBusAndNotifications - CMMC2-EventAuditingRules AWS Compliance Checks: <ul style="list-style-type: none"> - cmmc2-cloudtrail-without-log-file-validation - cmmc2-account-with-cloudtrail-disabled 	✓	✓

Excerpt from Our CMMC Control Matrix

Ensure Flexibility and Specificity

Kion makes it easy to bundle a set of CMMC level- specific controls into Cloud Rules to apply to relevant areas in your organization. Cloud Rules deliver the targeting you need to ensure a compliant foundation and put only the affected IT systems, rather than the entire corporate infrastructure, through the CMMC regime. You can configure your existing environment or build a new environment to meet your target CMMC level. In addition, you can:

- Apply checks only where you need
- Run checks on your own
- Write your own rules and compliance
- Go beyond our built-in engine by connecting with an external compliance

Achieve a Culture of Continuous Compliance

Compliance is an ongoing need and team members play a crucial role in meeting this need. Kion allows for continual compliance for your cloud resources, allowing you to monitor and prevent changes in resources or policies that can cause compliance drift. With Kion, you give all team members visibility into your compliance posture and help promote a cyber-aware and cyber-resilient culture. This is the smart direction for organizations as threats persist and the tolerance for cloud mishaps decreases.

Are you ready to take the next step? [Request a demo](#) with one of our cloud experts to see continuous compliance in action and discover how it will help you meet CMMC requirements now and in the future.

REQUEST A DEMO