Kion

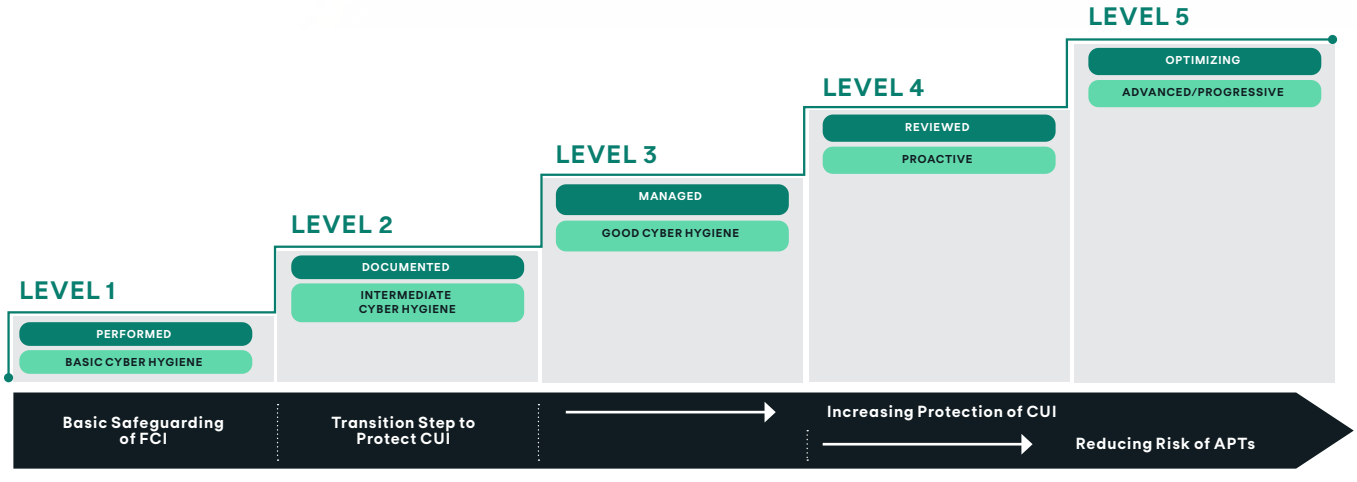
Get Ready for CMMC Today

And Achieve Continuous Compliance for the Future

The Steady Approach of CMMC

The Cybersecurity Maturity Model Certification (CMMC) framework consists of cybersecurity best practices and maturity processes. 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 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 five 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 5. Requirements at these levels will be familiar to many organizations. For example, CMMC Level 3, which is designed for federal contractors who process and store CUI, 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.



Source: Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC

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. By FY 2026, all DoD contracts are expected 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.

Difficulties of Ensuring 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 Level 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.[1]

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. Now, the introduction of CMMC requirements adds the potential inability to compete for contract awards as a ramification of failed audits.

Kion helps you overcome these cloud compliance difficulties.

Kion Eases the Path to 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 sunsetting—while enforcing access control and financial and compliance policies in the cloud.

Kion provides four key capabilities to deliver continuous compliance.

1. PREVENT

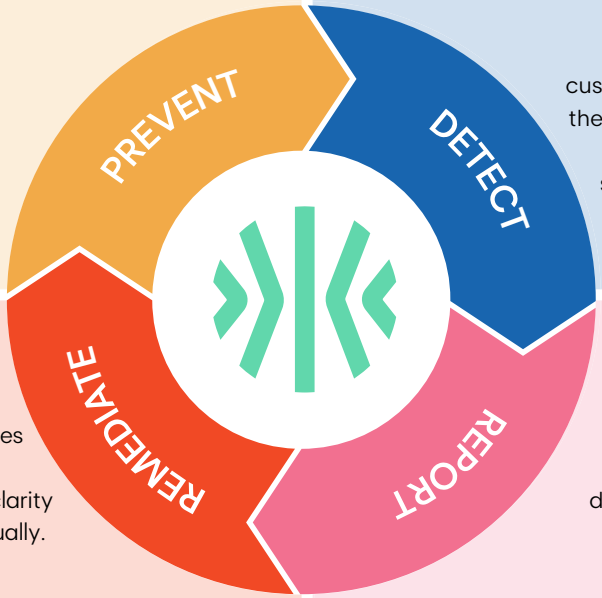
Compliance Rules:

Establish boundaries to prevent non-compliance with cloud rules. Use our compliance jumpstarts, which consist of plug-and-play cloud rules, to enforce policy with minimal configuration.

2. DETECT

Compliance Checks:

Continuously monitor your cloud with customizable compliance checks. Apply these checks only where you need them, conducting scheduled and manual scans for 24/7 coverage. We provide many checks to get you started.



4. REMEDIATE

Compliance Automation:

Enable automatic remediation of issues to fix compliance findings without manual intervention. Gain the visual clarity to find and address other issues manually.

3. REPORT

Compliance Dashboard:

Keep eyes on the compliance gap with clear visual indicators on the dashboard. Track violations found and addressed and sort by compliance standard (such as NIST or CIS).

1. https://go.logicworks.com/2019-state-of-aws-azure-cloud-compliance

Using Kion to Achieve CMMC

ASSESSING YOUR CURRENT MATURITY LEVEL

First, you must determine where you fall on the CMMC five-level maturity rating.[2] Most contracts are expected to specify Level 3 or lower, and the Level 3 requirements are expected to 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.

USING THE KION CMMC JUMPSTART

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 – 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 includes resources such as AWS IAM policies, CloudFormation templates, and Microsoft Azure managed policies. 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 all five levels of CMMC. At Level 3, Kion provides 93% addressable coverage of required controls.

CUSTOMIZING 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.

2. https://www.acq.osd.mil/cmmc/draft.html

To support CMMC V1.02, Our jumpstart includes:

- ✓ 129 AWS compliance checks
- ✓ 12 AWS CloudFormation templates
- ✓ 9 AWS IAM policies
- ✓ 9 Azure ARM templates
- ✓ 10 Azure policies
- ✓ 3 Azure roles
- ✓ 522 Azure managed compliance checks (58 for Azure Gov)
- ✓ 1 compliance standard containing all checks
- ✓ A yaml file to help you automate and expedite the creation of your System Security Plan (SSP)
- ✓ A 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

The Value of Kion Compliance

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 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 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 'audit 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	Ct Platform	CSP Platform	Audit Asset
AUDIT AND ACCOUNTABILITY	AU.3.051	AU.3.051	3	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. • NIST SP 800-171 Rev 1 3.3.5 • CIS Controls v7.1 6.6, 6.7 • NIST CSF v1.1 DE.AE-3 • CERT RMM v1.2 COMP: SG3.SP1 • NIST SP 800-53 Rev 4 AU-6(3)	AWS AWS Compliance Checks: - cloudwatch-alarm-without-actions - account-without-security-hub-enabled Azure Azure Managed Compliance Checks: - Microsoft Managed Control 1118 - Audit Review, Analysis, And Reporting | Correlate Audit Repositories	✓			✓

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 them.
- Run checks on your own timeline.
- Write your own rules and compliance checks.
- Go beyond our built-in engine by connecting with an external compliance engine.

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.

Get Started

Learn more about continuous compliance to help you meet CMMC requirements and be best prepared for ongoing compliance in the cloud.

Ready to get started? Contact our team for a demo of continuous compliance.

REQUEST A DEMO