KRATOS®
READY FOR WHAT'S NEXT™

Kratos Cybersecurity Maturity Model Certification (CMMC) Advisory Services

Kratos Cybersecurity Maturity Model Certification (CMMC) Advisory Services

Kratos' CMMC Advisory Services apply our insights and experience in support of providing reliable, CMMC-compliant and audit-defensible documentation packages that minimize risk. Kratos is an industry leader in providing repeatable, standardized, and audit-ready policies, procedures, plans, and processes that meet CMMC security practice and maturity requirements across all levels. Our 15-plus years as a leading provider of comprehensive cybersecurity solutions, addressing all aspects of the information security spectrum – from continuous monitoring and cloud security to risk management and compliances – provides the expertise necessary to achieve CMMC compliance.

The most significant benefit to partnering with Kratos is that doing so greatly reduces the risk of compliance failures that could potentially impact an ability to support Department of Defense (DoD) contracts. Kratos' goal is to establish a long-term partnership with our customers by providing immediate, future, and continued success. With this goal in mind, we bring the following key differentiators and unique features to the forefront of our advisory services:

- **Commercial-to-Government Compliance Experience:** As the current security advisor or assessor for many of the largest and most innovative commercial cloud service providers, we are very familiar with DoD expectations through our support of similar commercial-to-government compliance frameworks such as the Federal Risk and Authorization Management Program (FedRAMP) and Defense Security/Cybersecurity Authorization Working Group (DSAWG) cloud connection requirements.

- **Subject Matter Expertise across Compliance:** Kratos has worked alongside commercial and government organizations for many years advising, implementing, and assessing security parameters across a multitude of cybersecurity frameworks. Our experience across a full range of cybersecurity compliance frameworks and lifecycle integration enables our subject matter experts to pinpoint overlap within complementary security controls that allow customized frameworks focused on the best solutions. The key benefit is that all staff are cross-trained to support multiple compliance frameworks in both the assessor and advisor roles, providing the highest level of support.

- **Customer Focused Support Structure:** Kratos' support focuses on three key areas to enable continued customer success. Managing the day-to-day communications and activities across the people, processes and technologies requires efficient executive of service that cater to our customer's needs

What We Have Seen So Far

Our experience with CMMC has illuminated certain challenges. Some of these challenges are related to the fact that, as of this writing, the CMMC is not final. The CMMC Accreditation Body (CMMC-AB) has initiated the accreditation process for CMMC Third Party Assessment Organizations (C3PAO), which Kratos is currently undergoing. Leveraging these expert resources will prepare your organization for an eventual CMMC assessment of compliance requirements and accelerate time to certification.

Kratos is in communication with the CMMC-AB and is closely monitoring their activities as they move toward finalizing the CMMC requirements. The lack of finality presents the following challenges with regard to clarity:

- **Reciprocity:** it is unclear what level of reciprocity will exist between CMMC and other compliance frameworks.

- **Requirements:** the assessment requirements are not yet known. Similarly, while comprehensive drafts of CMMC-specific requirements exist – particularly present in Levels 4 and 5 – they are not final and therefore are subject to change.

- **Certification Level:** anticipating the level of certification required ahead of a Request for Proposal (RFP) is unclear. A good rule of thumb does exist, however: if the RFP involves CUI, at least a Level 3 certification is likely, while any RFP that doesn't involve CUI likely only requires either a Level 1 or 2 certification.

Throughout our CMMC engagements, we've seen additional challenges related to needs of organizations seeking certification, their boundary definitions and operational, technical and documentation requirements.

CMMC Boundary

Meeting with businesses on a daily basis, a question about the CMMC boundary always comes up. Prior to seeking certification, an organization must define the certification boundary. How an organization defines their boundary is integral to determining the certification scope, cost and level of effort. Organizations maintain latitude to define their boundaries in one of the following ways:

1. The entire organization
2. A program, business unit or isolated environment within the organization

If an organization seeks certification for their entire organization, the scope, cost and level of effort can be significant, particularly if the organization is large and is seeking a Level 3-5 certification. Furthermore, implementation of certain Level 4 and 5 requirements is not practical on an organization-wide scale. For most organizations, an organization-wide certification only makes sense at either Level 1 or 2. Alternatively, if an organization seeks certification of a program, business unit or isolated environment, scope, cost and level of effort are significantly less than the organization-wide approach, particularly as the certification level increases.

Strategic and Operational Challenges

Throughout our CMMC engagements, we've identified requirements that impose strategic and operational challenges on organizations seeking certifications of Level 3 or higher:

Strategic Challenges

- **Centralization:** Many organizations have similar tools that perform the same function, or the same tools that support different groups. This creates blind spots within the organizations and makes it difficult to understand the true risk posture of the organization. Consolidating resources where redundancies exist, and providing a common centralized repository for approved processes, technologies and software made available throughout the organization will enable the organization to implement needed changes faster and more reliably.

- **Documentation:** Many organizations are familiar with the documentation required for any number of compliance frameworks; however, the CMMC requires a much more robust documentation ecosystem than we've seen across all others. Organizations need to conduct a thorough review of existing documentation, providing enhanced updates that include requirements specifically defined in the CMMC framework. Furthermore, develop a strategy and process that ensures consistent and effective communication of documentation throughout the organization.

- **Exceptions:** Develop a repeatable, trackable and documented process to handle inevitable deviations from baseline standards. If the process is too difficult to follow, people will find another way. Deviations from the standards are not a bad thing, so long as they are known and measures have been established to provide compensating security that reduces risk.

- **Acquisitions:** For larger organizations, acquisitions are a common occurrence and a mechanism for business and capability growth. We have seen it take years to fully integrate new acquisitions, and this period of transition can create great risk within the organization. Establishing a clearly structured strategy to integrate IT and security for new and existing acquisitions is critical.

- **Supply Chain Risk Management:** While many organizations are attempting to become CMMC compliant themselves, it is important that members of your supply chain are not forgotten. Establishing a defined strategy to manage risk associated with the overall supply chain that includes subcontractors and suppliers, will require cooperation across multiple areas of the business outside of security. Beginning conversations and outreach early has proven to be an important step to help your business critical partners become CMMC ready.

Operational Challenges

For organizations that process, store, transmit, and protect CUI, you will need to meet CMMC Level 3 as a minimum standard. Out of the 130+ security practices an organization will be required to meet, many of our customers find that the following six (6) operational challenges are the most difficult, time consuming, or cost concerning requirements. If not already implemented, these will require the longest lead time and/or changes to the organization's security culture.

1. **Vulnerability and Patch Management:** Ensure that vulnerability scans are conducted on all operating systems, databases and applications through the organization. Similarly, establish and communicate defined remediation times and provide consistent patching across all systems.
2. **Identity and Access Management:** Implement multi-factor authentication for all privileged and non-privileged access to the environment accompanied by regularly scheduled reviews of access privileges.
3. **Encryption:** Implement FIPS 140-2 validated cryptographic modules to protect data in transit and at rest.
4. **Auditing:** Define required audit log content, ensure the defined content is sent to a centralized repository and configure automated alerts for specified failures and indicators of compromise.
5. **CUI Marking and Handling:** Establish guidelines and procedures to ensure that CUI is marked and handled in accordance with CMMC and contractual requirements
6. **Allow Lists/Block Lists:** Establish the use of either an allow list or block list. Enforce the allow list or block list throughout the organization to prevent the use of unauthorized software.

In addition to the strategic and operational challenges discussed above, organizations must consider the possibility that they may require certification at multiple levels of CMMC. We recommend that organizations seek the certification that aligns with the highest anticipated level, based on current and future engagements with the DoD. Planning ahead provides a better roadmap for distributing the workload over time to achieve what CMMC level is needed now and in the future.

Documentation

CMMC's documentation requirements are significant. Policy and procedure documents are required for each of the 17 domains, while additional plans are required, depending on the certification level.

There are currently no official templates for the many documents required for a CMMC certification. Kratos has developed templates that are tailored specifically to CMMC requirements and provide straightforward traceability to the CMMC Capabilities and Practices.

A Successful CMMC Approach

Unlike most organizations offering CMMC Advisory services, Kratos is a large contributor and partner with the Defense Industrial base (DIB). As a result, we have a unique understanding and insight into how the CMMC requirements impact DIB organizations and what can and/or should be done to satisfy those requirements. Rather than the typical "cookie-cutter" approach to compliance taken by most Advisory companies, Kratos has tailored our approach, using our extensive knowledge gained as a member of the DIB, to address the DIB-specific issues and pain points in meeting the non-DIB-specific compliance framework.

Given that CMMC is not final, the current focus and approach to CMMC is one of readiness. Our advisory services can identify areas for improvement on the CMMC readiness path and assist with implementation of identified improvements. Our services are designed to meet the needs of our customers by providing a range of support models that can be fully customer-integrated and hands on or ad hoc consulting. Three of the most common services that we are providing today, include:

Strategic & Operational Consulting

Our strategic and operational consulting services help organization prepare for specific CMMC certifications and readiness efforts. We provide general guidance, answer questions and serve as a partner in determining the CMMC boundary, level of certification, scope and level of effort. These services provide on-demand support to answer questions, provide guidance, and review information. For this service, an organization is provided with a primary technical point of contact that organizations can reach to for support. Coupled with the primary POC, organizations will also have reach-back capability to the rest of our subject matter experts that can be utilized for specific needs.

Gap Assessment

Our Gap Assessment provides a review an organization or environment against each of the defined CMMC level requirements, including review and analysis of all applicable security practices and process maturity controls to determine compliance, identify gaps, and provide recommendations. The outcome of the assessment is an evaluation of an organization's or environment's compliance posture relative to CMMC standards through interviews, observation and documentation review.

- **Documentation Review:** We'll collect policies, procedures, architectural diagrams, functional specifications and other relevant documents to determine if the organization or environment is meeting practice requirements.

- **Interviews and Observation:** We'll conduct interviews and observe evidence to gain greater insight into the organization or environment to determine compliance with CMMC practice requirements.

- **Sampling Methodology:** Gap assessments are typically conducted across the entirety of an organization or environment; however, in certain instances a more cost effective approach is to employ sampling Sampling is only an option for organizations or environments with rigid change management processes and highly automated mechanisms for implementing CMMC solutions across large, geographically dispersed production environments.

- **Data Analysis and Reporting:** The final phase of a gap assessment, in which the results are documented and distributed. The identified gaps are associated with one of the following focus areas: Documentation, Process and Operations or Engineering and Technology, with high priority, high impact issues specifically highlighted.

Documentation Services

Our documentation services focus on development of CMMC-compliant documentation to satisfy the application certification level requirements. Our services include developing policies, procedures, plans and/or other supporting documentation to address requirements for all applicable security practices and maturity model controls.

- **Data Gathering:** We'll use a five-step process to develop CMMC documentation:

1. **Incorporate Existing Documentation:** Transpose existing documentation into CMMC-compliant formats.
2. **Identification of Undefined CMMC Security Practice Parameters:** Identify all organizationally-defined security parameters that are undefined within existing documentation.
3. **Identification of Missing CMMC Security Elements:** Identify additional security elements that the organization must define.
4. **Security Practice Working Sessions:** Utilizing the items identified in Steps 2-3, conduct working sessions to gather the necessary information and incorporate into relevant documentation
5. **Identification of Non-Compliant CMMC Security Practices:** Identify non-compliant areas that require further resolution.

- **Documentation and Reporting:** Drafting and finalization of the following documents:

Level 2:
- Policy for each of the 17 domains
- Procedure for each of the 17 domains
- Configuration Management Plan
- Incident Response Plan
- Contingency Plan
- Risk Mitigation Plan
- Vulnerability Management Plan
- System Security Plan

Level 3:
- Level 2 documentation
- Resource Plan for each of the 17 domains
- Separation of Duties / Privilege Functions Matrix
- Business Impact Analysis
- Continuous Monitoring Plan

Level 4:
- Level 2 & 3 documentation
- Supply Chain Risk Management Plan
- Penetration Testing Plan
- Red Teaming Plan

Why Kratos

Many organizations have already initiated efforts to meet the demanding requirements of the CMMC framework. Kratos' current customer base includes cloud-native and traditional on-premises environments, both large and small. Selecting an experienced and proven CMMC partner is critical to enable an organization's CMMC success in an efficient and timely manner. This includes partnering with someone that has experience with both large and small organizations, where solutions and cost are critical factors. In addition to our current CMMC support, Kratos has years of compliance and government certification experience and deep expertise in advising government agencies and commercial organizations on compliance requirements including the Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), and National Institute of Standards & Technology (NIST)/ Risk Management Framework (RMF) and the Federal Risk and Authorization Management Program (FedRAMP). As one of the industry's leading FedRAMP 3PAOs, we will be among the first accredited to become a CMMC 3PAO, ready to assist all types of organizations with CMMC advisory or assessment service needs.

About Kratos

Kratos Defense & Security Solutions, Inc. (NASDAQ:KTOS) develops transformative, affordable technology for the Department of Defense and commercial customers. Kratos is changing the way breakthrough technology for these industries are brought to market through proactive research and a streamlined development process. Kratos specializes in unmanned systems, satellite communications, cyber security/warfare, microwave electronics, missile defense, training and combat systems. For more information, go to www.KratosDefense.com.

KRATOS®
READY FOR WHAT'S NEXT™

HEADQUARTERS
Kratos Defense & Security Solutions
10680 Treena Street
6th Floor
San Diego, CA 92131

Cybersecurity Solutions
Kratos
4795 Meadow Wood Lane
Suite 220W
Chantilly, VA 20151
Phone: 888.677.9351
CyberSales@KratosDefense.com