Responding to Issues Organizations Face in Compliance with the Cybersecurity Maturity Model Certification (CMMC)

Common Issues and Concerns Organizations Face in Compliance with the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)

*Kratos Cybersecurity Services is pleased to provide you this **Common Issues and Concerns Organizations Face in Compliance with the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)**. Fifteen-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 foundation for our expertise in CMMC compliance.*

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 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 Controlled Unclassified Information (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, including their boundary definitions and operational, technical and documentation requirements.

CMMC Boundary

Meeting with businesses on a daily basis, the question about the CMMC boundary continually arises. 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

During our CMMC engagements, we've identified common requirements that impose strategic and operational challenges on organizations seeking certification at 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 organization and makes it difficult to understand the true risk posture of the organization.
  - Consolidate resources where redundancies exist, and provide 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.
  - Conduct a thorough review of existing documentation, providing enhanced updates that include requirements specifically defined in the CMMC framework.
  - Develop a strategy and process that ensures consistent and effective communication of documentation throughout your organization.

- **Exceptions:** Develop a repeatable, trackable and documented process to handle the inevitable deviations from CMMC 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 controls that reduce risk.

- **Acquisitions:** For larger organizations, acquisitions are a common occurrence and a mechanism for business and capability growth. In some cases, it takes years to fully integrate new acquisitions into the larger organization, and this period of transition can create great risk within the organization.
  - Establish a clearly structured strategy to integrate IT and security for new and existing acquisitions. This is a critical step

- **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.
  - Establish a defined strategy to manage risk associated with the overall supply chain that includes subcontractors and suppliers. This 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 you will be required to satisfy, 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 your security culture.

- **Vulnerability and Patch Management:** Ensure that vulnerability scans are conducted on all operating systems, databases and applications throughout the defined CMMC boundary. Similarly, establish and communicate defined remediation times and provide consistent patching across all systems within the defined CMMC boundary
- **Identity and Access Management:** Implement multi-factor authentication for all privileged and non-privileged access to information systems and network resources within the defined CMMC boundary accompanied by regularly scheduled reviews of access privileges.
- **Encryption:** Implement FIPS 140-2 validated cryptographic modules to protect data in transit and at rest.
- **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.
- **CUI Marking and Handling:** Establish guidelines and procedures to ensure that CUI is marked and handled in accordance with CMMC and contractual requirements.
- **Allow Lists/Block Lists:** Establish the use of either an allow list or block list. Enforce the allow list or block list throughout the defined CMMC boundary to prevent the use of unauthorized software.

In addition to the strategic and operational challenges discussed above, you should consider the possibility that you may require certification at multiple levels of CMMC. We recommend that you 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.

A Successful CMMC Approach

Given that CMMC is not final, the current primary focus and approach to CMMC is one of readiness. You should be proactively identifying areas for improvement on the CMMC readiness path and develop plans and strategies for the implementation of identified improvements.

Strategic & Operational

Particular focus needs to be on determining the CMMC boundary, level of certification, scope and level of effort. As stated above, prior to seeking CMMC certification, you will need to define the certification boundary. How you define your boundary is integral to determining the certification scope, cost and level of effort.

Gap Assessment

Gap Assessment provides a view an organization or environment against each of the defined CMMC level requirements within the defined CMMC boundary. The Gap Assessment should include a review and analysis of all applicable security practices and process maturity controls to determine compliance, identify gaps, and develop strategies and plans for any required remediation.

Documentation

Focus also needs to be placed on the development of CMMC-compliant documentation to satisfy the application certification level requirements within the defined CMMC boundary. You need to ensure you have policies, procedures, plans and/or other supporting documentation to address requirements for all applicable security practices and maturity model controls.

Your documentation efforts should include revising or creating 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 / Privileged 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

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