Hypori

Cybersecurity Maturity Model Certification (CMMC) Industry Insights

Challenges & Strategies

Industry Insights

Challenges & Strategies

Cole French
Director of Cybersecurity Services, Kratos Defense and Security Solutions
LinkedIn

carahsoft.

For more information, contact Carahsoft or our reseller partners:
Hypori@carahsoft.com | 571-622-4800

Hypori

Thank you for attending this Hypori's hybrid event! Carahsoft is the distributor for Hypori CMMC solutions available via NASA SEWP V, Department of General Services Pennsylvania, Educational Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring Hypori's solutions, please check out the following resources and information:

For additional resources:

carah.io/HyporiResources

For additional Hypori solutions:

carah.io/HyporiSolutions

To purchase, check out the contract vehicles available for procurement:

carah.io/HyporiContracts

For upcoming events:

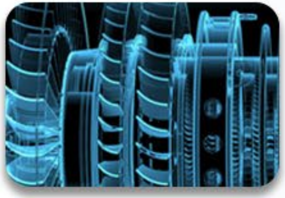
carah.io/HyporiEvents

For additional CMMC solutions:

carah.io/CMMCSolutions

To set up a meeting:

Hypori@carahsoft.com or 571-662-4800



KRATOS
READY FOR WHAT'S NEXT™

Cybersecurity Maturity Model Certification (CMMC)

Industry Insights

Challenges and Strategies

CMMC Accelerate | Carahsoft Conference & Collaboration Center

Herndon, VA | March 13, 2025

Agenda

- Kratos – Who We Are
- State of the Ecosystem
- Strategies
- Assessments (So Far)
- What's Ahead
- How to Help Your Assessor

Kratos – Who We Are

- Kratos builds technology and other products supporting strategic and transformational national security programs
  - ❑ Unmanned systems
  - ❑ Assured aerospace communications
  - ❑ Cybersecurity (FedRAMP 3PAO, CMMC C3PAO, RPO, and Advanced Cyber Services)
  - ❑ Strategic programs
  - ❑ Microwave electronics
  - ❑ Training and simulation

State of the Ecosystem

- The 32 CFR (Program Rule) was published on October 15, 2024
- Phased implementation extended
- Applicability of CMMC to External Service Providers clarified
- FedRAMP equivalency requirements are unchanged, but applicability updated for Security Protection Assets
- Assessment Team composition requirements defined
- Assessment scoring and POA&M eligibility defined
- Quality Assurance requirements defined
- **Contracting officers <u>can</u> write CMMC requirements into contracts <u>today</u>**

Strategies – Scope

- At the most basic level, the scope is what’s being evaluated
- Define the assets in scope (people, processes, and technologies)
- Remember those things you forgot
  - ❑ Data flows are part of your scope
  - ❑ Automation can be helpful
- Leverage the CMMC scoping guide
- If you’re not confident in your scope, keep working at it

Strategies – Auditing

- Need to capture from a potentially wide-range of endpoint types
- Defined audit events for capture (broader the better)
- Detection and notification of logging failures (prove the negative)
    - ❑ Failure of an endpoint to audit events
    - ❑ Failure to process an endpoint’s logged events
- Reporting, correlation, and reduction capabilities
- Audit log reviews and analysis (reviewing auditable event types and reviewing audit events are not the same thing)

Strategies – Those Things That Haven’t Happened Yet

- Common things we’ve assessed that haven’t happened yet
  - ❑ Emergency changes
  - ❑ Security incidents
  - ❑ Termination or transfer of users
  - ❑ Documentation reviews
  - ❑ Removing material that shouldn’t have been posted publicly
- Process, Process, Process (in documentation, of course)
- Testing is a great practice to demonstrate *how* these *would* be handled

Strategies – POA&Ms

- Understanding what a POA&M actually is (and isn't)
    - ❑ An integral part of maintaining any system
    - ❑ More just vulnerabilities
    - ❑ Key component of maturity, as it tells a story of the system
    - ❑ It is <u>not</u> the outcome of an assessment
- An empty POA&M is problematic
    - ❑ No system has zero vulnerabilities
    - ❑ Part of managing a system should include <u>identifying areas for improvement</u>
- Leveraging automation can be helpful

Strategies – Risk Assessments

- A security control assessment is not a risk assessment by itself
- Vulnerability scanning is not a risk assessment by itself
- Evaluating security configuration settings is not a risk assessment by itself
- Comprehensive risk assessments must evaluate risks to the business and mission and determine the likelihood of their occurrence
- The activities above can be components of risk assessments
- More importantly, the activities above can be informed by risk assessments, which enables targeted risk reduction

Strategies – Defined Frequency

- Organizationally defined frequencies cannot exceed 1 year
- Don’t use ‘frequently’
- Don’t use ‘occasionally’
- Don’t use ‘periodically’
- Don’t use ‘sometimes’
- Don’t use ‘every three years’
- Be specific, but also give yourself wiggle room (e.g., “a period not to exceed 30 days”)

Assessments (So Far)

- CMMC Assessments began on January 2, 2025
- The Certificate of Status was released for use on March 7, 2025
- ‘Continuous monitoring’ is an annual attestation of compliance
- Enclaves can make it easier (especially VDI)
- Organization and role definition are important
- The queue is growing steadily

What’s Ahead?

- Assessments, assessments, assessments (but maybe not so fast)
- Title 48 CFR will trigger Phase 1 of the implementation
- The mechanics of the program
- FedRAMP Equivalency updates
- Enclaves look more and more appealing
- Stronger focus on implementing ‘make-or-break’ controls
- Assessor interpretations highlight the need for strong preparation

How to Help Your Assessor

- Finish your SSP (no, really)
- Documentation matrix
- Clearly define external service provider relationships
- Shared Responsibility Matrices
    - ❑ Understand them (really)
    - ❑ They’re needed for more than just cloud service providers
- Leverage inheritance properly (e.g., don’t regurgitate material from a provider’s SSP in your SSP)