The **Cybersecurity Maturity Model Certification** draft final rule is out. Now what?

5 key requirements to monitor on your journey

1 Addressing Plan of Action and Milestones (POA&M) items

Final Joint Surveillance Voluntary Assessment (JSVA) audit status will not be awarded until all open POA&M items are addressed. POA&Ms must be remediated within 180 days of assessment.

Why it matters
This requirement creates challenges for cybersecurity personnel, including increased workload and pressure from leadership for quick resolution and resource constraints, affecting thorough analysis and implementation of effective security measures.

What can you do?
If you have already completed a JSVA or are planning to sit for one soon, review your POA&M to ensure timely remediation. Consider assistance from a qualified resource like RSM to help expedite remediation activities.

2 Managed services provider (MSP), external services provider (ESP) and managed security services provider (MSSP) certification requirements

If an organization seeking certification (OSC) uses an MSP, ESP and/or MSSP, the provider must have their final certification levels at the level required by the OSC prior to the OSC seeking certification.

Why it matters
An MSP, ESP or MSSP may not be as mature in the certification journey as an OSC or may be planning to attain certification prior to the OSC seeking certification.

What can you do?
Validate the certification status of MSPs, ESPs and MSSPs within boundaries and enhance or enforce third-party vendor and risk management practices to track and monitor MSP/ESP/MSSP compliance. Not sure how to get started? RSM's third-party risk management services team can develop a plan to manage your process.

3 New affirmation requirements for Level 1, 2 and 3 maturity assessments

Senior leadership at OSCs are required to sign and attest to the validity of any assessment or POA&M closeout and to do so annually moving forward.

Why it matters
Ambiguities in defining "senior leadership" for attestation and limiting accountability only to individuals such as chief information security officers may create challenges for cybersecurity personnel.

What can you do?
OSCs should begin reviewing responsible and accountable roles for their CMMC journey and designate officials for affirmation statements. Not sure how to get started? RSM provides advice and services to strategically align your organization's CMMC journey and business to support strategy moving forward.

4 Operational technology (OT) cybersecurity requirements

While the rule will affect OT environments in the defense industrial base (DIB) the draft final rule does not offer updates on how they are to be "documented but not assessed" against CMMC security requirements.

Why it matters
The discrepancy between the requirement for documentation of OT in inventory, the system security plan and the network diagram, and the absence of a direct assessment against CMMC requirements raises questions about the effectiveness of this scoping decision.

The lack of direct assessment against CMMC requirements for OT and specialized assets could result in an incomplete understanding of potential vulnerabilities affecting the DIB.

What can you do?
Perform readiness activities on OT environments to determine potential vulnerabilities in your organization.

5 Operational and financial planning

Categorization of CMMC costs (nonrecurring engineering, recurring engineering, assessment, affirmation) requires careful financial planning for organizations—with the Department of Defense's assumption that Levels 1 and 2 are already implemented throughout the DIB.

Why it matters
This requirement introduces financial considerations, potentially affecting resource allocation for achieving higher CMMC levels.

The substantial cost estimate for CMMC Level 2 (more than $100,000) raises financial concerns, especially for smaller contractors, necessitating exploration of cost mitigation strategies.

What can you do?
Perform strategy and operational planning assessments to review and assess potential increases or decreases in operational costs associated with CMMC compliance.

Reach out to RSM to explore cost recovery strategies.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

ig_0324_cmmc infographic