Attain. Maintain. **Prove it Anytime.**

Breaking it Down: Why CRMAs Must Implement NIST SP 800-171 Requirements

Clarifying CRMA Obligations and Assessment Expectations

Written By: Rachel Leidy, Director of Compliance Education, CCA, CCP, CISSP

This position article addresses common misunderstandings surrounding Contractor Risk Managed Assets (CRMAs). Effectively managing CRMAs is crucial for organizations striving to comply with NIST SP 800-171 Level 2 requirements under the Cybersecurity Maturity Model Certification (CMMC). While CRMAs are not intended to process, store, or transmit Controlled Unclassified Information (CUI), their proximity to CUI environments presents inherent risks. This article clarifies compliance expectations, emphasizing comprehensive documentation, and readiness for assessments to mitigate risks associated with interconnected assets.

Table of Contents

1. Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) framework mandates that all Contractor Risk Managed Assets (CRMAs) implement National Institute of Standards and Technology (NIST) Special Publication (SP)800-171 Level 2 requirements. CRMAs are defined as assets that can, but are not intended to, process, store, or transmit CUI, as restricted by organizational policies, procedures, and practices.

The Department of Defense (DoD) introduced the CRMA category to reduce assessment burdens by accepting the risk of not performing a full assessment on these assets, provided the organization can restrict CUI interaction through well-documented policies, procedures, and practices. Nonetheless, these assets must still comply with Level 2 security requirements to safeguard CUI and mitigate risks such as unauthorized access or data leakage.

This article outlines:

- The purpose of the CRMA asset categorization.
- The rationale for applying NIST SP 800-171 controls to CRMAs.
- CRMA assessment expectations.
- The meaning of organizational policies, procedures, and practices.
- The critical role of the System Security Plan (SSP).
- What organizations can expect during a limited spot check for CRMAs.
- Tips for CRMA assessment preparation.

By following the guidelines outlined in this article, contractors can align with DoD expectations, reduce risks, and strengthen compliance practices.

2. CRMAs Must Implement Level 2 Controls

CMMC mandates that CRMAs implement all NIST SP 800-171 Level 2 controls, even if these assets are not intended to process, store, or transmit CUI. This requirement is grounded in regulatory text, logical security rationale, and the overarching need to maintain a robust cybersecurity posture for all assets within the security boundary. The following elaborates on the regulatory basis and logical justification for securing CRMAs to the same standard as CUI assets.

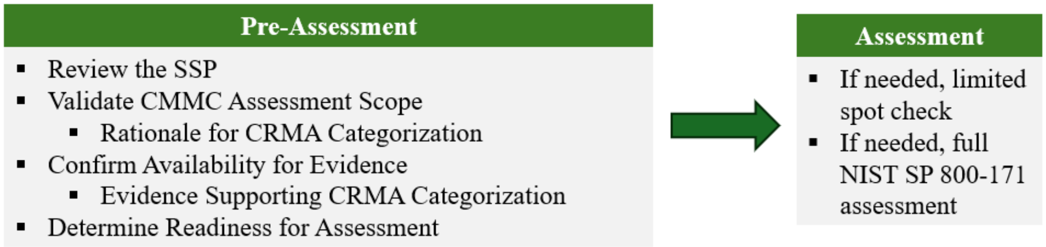
2.1. Regulatory Basis and References

- **Preparation:** The CMMC rule explicitly states that CRMAs must be "prepared to be assessed against CMMC security requirements at Level 2". This preparation inherently requires implementing Level 2 controls on CRMAs (https://www.federalregister.gov/d/2024-22905/p-695).
- **Level of Protection:** While the CRMA category aims to reduce assessment burdens, the rule emphasizes that this categorization "is not intended to reduce the level of protection" required for these assets (https://www.federalregister.gov/d/2024-22905/p-694).
- **Must be Met:** When an organization designates an asset as CRMA, all Level 2 security requirements must be fully implemented, and self-assessed as met, to ensure these assets meet the necessary compliance and security standards, regardless of their intended restricted interaction with CUI (https://www.federalregister.gov/d/2024-22905/p-696).
- **Risk Tolerance and Limited Checks:** The DoD has accepted the risk of conducting limited checks on CRMAs instead of full assessments because these assets are not intended to handle CUI. Limited checks verify compliance with organizational policies, procedures, and practices. Organizations should be prepared for these assessments, as any deficiencies or concerns identified by assessors could prompt a deeper evaluation of CRMAs against applicable Level 2 requirements (https://www.federalregister.gov/d/2024-22905/p-706).

2.2. Logical and Security-Based Rationale

CRMAs that exist within the same network environment as CUI assets without logical or physical separation, pose inherent risks such as unauthorized access, lateral movement, and data leakage if safeguards fail. Basic cybersecurity principles emphasize that all assets within a security boundary must maintain consistent levels of protection to mitigate interconnected risks. Adversaries often target less-secured assets in an environment to gain a foothold and bypass stricter protections on critical assets, like CUI assets. By implementing robust Level 2 controls on all interconnected assets and adhering to the principle of defense-in-depth, organizations create multiple layers of security, reducing the likelihood of lateral movement, privilege escalation, or other potential vulnerabilities.

3. CRMA and the Assessment Process



Pre-Assessment

- Review the SSP
- Validate CMMC Assessment Scope
  - Rationale for CRMA Categorization
- Confirm Availability for Evidence
  - Evidence Supporting CRMA Categorization
- Determine Readiness for Assessment

Assessment

- If needed, limited spot check
- If needed, full NIST SP 800-171 assessment

During a CMMC assessment, assessors utilize three primary methods to evaluate compliance: **examine**, **interview**, and **test**.

For CRMAs, the examination and interview methods are the primary focus during the pre-assessment phase. Assessors examine documentation such as the SSP, network diagrams, asset listings, and organizational policies, procedures, and practices to validate that CRMAs are properly categorized and managed. These documents must clearly demonstrate how CRMAs are restricted from processing, storing, or transmitting CUI.

Helpful Tip for FutureFeed Users

When categorizing assessment scope assets, remember to document your rationale for including and excluding assets from scope. FutureFeed's process walks you through asset categorization and helps ensure everything is properly documented for assessors, reducing the chance of confusion or follow-up questions. Use the mapping function to link documents and evidence.

In addition to documentation review (examine), assessors use the interview method during the pre-assessment phase. This involves engaging with the organization to understand how they scoped their environment, categorized assets, and their rationale for CRMA designations. These interviews provide critical context for assessors to evaluate whether the organization's categorization is accurate and sets the stage for how those assets will be handled during the assessment phase.

However, assessors will not typically perform the **test** method—testing control objective implementation—on CRMAs. A full assessment is not conducted unless issues arise, gaps or deficiencies are identified during a limited spot check, or an assessment scope change occurs. This limited approach reflects the DoD's intent in creating the CRMA category: to reduce assessment burdens by accepting the risk of not performing a full Level 2 assessment using all three assessment methods. This reduced burden is contingent on the organization's ability to restrict CRMA-CUI interaction through well-documented and enforceable security policies, procedures, and practices.

By adhering to these pre-assessment expectations and ensuring comprehensive documentation, organizations can effectively minimize the likelihood of deeper assessment or a scope change, thereby benefiting from the streamlined approach intended for CRMAs.

4. Organizational Policies, Procedures, and Practices

Organizational policies, procedures, and practices frame a contractor's compliance efforts under the CMMC framework. The rule states "Contractor's risk-based security policies, procedures, and practices are not used to define the scope of the assessment, they are descriptive of the types of documents an assessor will use to meet the CMMC assessment requirements" (https://www.federalregister.gov/d/2024-22905/p-698). This statement implies that "Organizational Policies, Procedures, and Practices":

- **Must Address NIST SP 800-171 Requirements:** They need to cover the security controls and requirements outlined in NIST SP 800-171 for all in-scope assets, including CRMAs.
- **Can Include Broader Security Measures:** These policies, procedures, and practices are not limited to NIST SP 800-171; they may also include additional security, operational, and risk management needs specific to the organization. For example:
  - Industry-specific compliance requirements (e.g., ITAR, ISO 27001).
  - Broader risk management strategies beyond the NIST framework.
  - Operational controls related to internal practices, physical security, or vendor management.
- **Assessment Focus:** The assessor focuses on the aspects of these policies and practices that relate to NIST SP 800-171 compliance during an assessment and CRMA categorization during the pre-assessment. These documents are not used to define assessment scope but rather validate compliance.

Helpful Tip for FutureFeed Users

Save time and ensure accuracy with FutureFeed's pre-built templates for policies, procedures, and practices. Each template is designed to meet NIST SP 800-171 and CMMC requirements while allowing customization for your unique environment.

4.1. The System Security Plan (SSP) and CRMAs

The SSP is critical in planning and maintaining security control implementation. If there is concern about the organizations ability to restrict CRMAs from processing, storing, or transmitting CUI due to lack of security policy, procedures, and practices and/or sufficient documentation, the assessor will move onto performing a limited spot check. The SSP should:

- **Facilitating Compliance:** Documenting control implementation method in the SSP provides a clear roadmap for compliance planning, identifying, and addressing potential compliance gaps, and supports organizational continuous monitoring activities.
- **Support Compliance Verification:** The SSP must clearly articulate the method of implementation for all NIST SP 800-171 Level 2 controls for in scope assets, including those applied to CRMAs.
    - Comprehensive and detailed documentation in the SSP is critical for assessors to evaluate compliance with asset categorization requirements. By clearly describing how security requirements are implemented, the SSP enables assessors to determine whether a limited spot check is necessary and if the organization has adequately met the conditions to exclude CRMAs from broader assessment requirements. Insufficient or unclear documentation may prompt assessors to initiate a limited spot check to validate compliance. Should deficiencies or gaps be identified during this process, the affected requirement could be scored as 'NOT MET,' potentially triggering an expanded assessment of additional controls (https://www.federalregister.gov/d/2024-22905/p-703).
    - This aligns with CA-3.12.4's assessment objectives, which require that the method of control implementation be "described or documented" (NIST SP 800-171A Rev 2). Without this level of detail, assessors cannot effectively verify compliance.
    - Note: All CMMC security requirements must be MET when the OSA chooses to designate certain assets as Contractor Risk Managed Assets (https://www.federalregister.gov/d/2024-22905/p-696).
- **Support Accurate Categorization:** Properly documenting how policies, procedures, and practices restrict CRMAs from interacting with CUI ensures accurate CRMA categorization and facilitates assessor verification.

5. What a Limited Spot Check May Consist Of

Limited spot checks verify that CRMAs are categorized and managed according to the SSP and documented policies, procedures, and practices. A finding of "Not Met" during a limited spot check will potentially trigger a deeper assessment (https://www.federalregister.gov/d/2024-22905/p-703).

- **Scope of Limited Spot Checks:** The checks are not meant to assess full compliance with all NIST SP 800-171 Level 2 controls for CRMAs. Instead, they focus on verifying whether the organization's controls adequately enforce the intended CRMA designation, as defined by the organization's documented policies and practices.
- **Evidence:** A limited check may involve the submission of evidence to demonstrate compliance with organizational policies, procedures, and practices that restrict CRMAs from processing, storing, or transmitting CUI (https://www.federalregister.gov/d/2024-22905/p-700).
- **Policy, Procedure, Practice Review:** Assessors will evaluate the documented policies, procedures, and practices supporting the CRMA designation to ensure they effectively restrict CRMAs from processing, storing, or transmitting CUI. For example:
    - Does the policy clearly state that CRMAs are prohibited from storing, processing, or transmitting CUI?
    - Are there procedures in place to enforce and audit this restriction?
- **Verification of Implementation:** Assessors may look for evidence that the policies, procedures, and practices are being implemented effectively. For example, this could include:
    - Evidence Acceptable Use Policy sign-off.
    - Interviews with personnel to confirm understanding and adherence to CRMA restrictions.

Helpful Tip for FutureFeed Users
Be ready for limited spot checks with FutureFeed's integrated assessment readiness tools. FutureFeed serves as your system of record, housing all documentation, evidence, and policies in one place for smooth, efficient assessments. Assessors will appreciate the enhanced evidence traceability FutureFeed provides.

- **Control Effectiveness Validation:** Assessors might assess specific controls related to CRMA documentation requirements and the CRMA categorization intent to ensure their functionality. For example:

- Access controls preventing CRMAs from connecting to CUI repositories.
- Network segmentation or other safeguards that limit CRMAs' interaction with CUI environments.

- **Deeper Dive:** If the limited spot check reveals deficiencies or raises concerns about the effectiveness of the controls, assessors may expand their evaluation to include other Level 2 requirements for the CRMAs in question (https://www.federalregister.gov/d/2024-22905/p-706).

6. Preparing for Assessments

6.1. Pre-Assessment Prep

To avoid compliance gaps or an expanded assessment, the following documentation is required and should support the categorization of CRMAs:

Helpful Tip for FutureFeed Users
FutureFeed is designed to guide you through every stage of assessment readiness. Look for the quick tips, reference guides, and instructional videos throughout the tool—strategically placed to help you with categorization, documentation, evidence preparation, and much more exactly when you need it.

- **SSP:** The SSP must document the method of implementation for all applicable NIST SP 800-171 Level 2 controls, including those applied to CRMAs. Include narratives and justifications for CRMA categorization, ensuring alignment with organizational policies and practices.
- **Network Diagram:** Provide a comprehensive network diagram that clearly indicates the placement and connections of CRMAs within the environment.
- **Asset Inventory:** The assessment scope asset listing should include all CRMA assets. Ensure the asset inventory aligns with the SSP and network diagram.
- **Applicable Policies:** Policies should clearly state that CRMAs are prohibited from handling CUI. For example:
  - An Acceptable Use Policy (AUP) might specify that CUI can only be stored, processed, or transmitted on designated assets, restricting CRMAs from these activities.
  - Include policies related to access control, acceptable use, and security categorization that reinforce CRMA restrictions.
- **Applicable Procedures:** Procedures must enforce the policies. For example:
  - Develop procedures for monitoring and auditing CRMA usage to ensure compliance and detect unauthorized CUI interaction.
  - Include incident response steps specific to CRMAs in case of policy violations or unauthorized access attempts.
- **Applicable Practices:** Practices should demonstrate how policies and procedures are operationalized. For example:
  - Provide evidence of routine staff training on CRMA restrictions and related organizational policies.
  - Document ongoing monitoring activities, such as logs or reports, which verify adherence to CRMA restrictions.
  - Include examples of corrective actions taken to address non-compliance, if applicable.

By ensuring these documents are thorough, consistent, and readily available, organizations can effectively demonstrate their compliance efforts, minimize the risk of a limited spot check or an expanded assessment, and validate the proper categorization of CRMAs.

6.2. Assessment Prep

To avoid compliance gaps and "Not Met" results during limited spot checks or a scope change with a full assessment, ensure the following:

- **SSP:** Plan for the implementation of all Level 2 controls and clearly document the method of implementation in the SSP. A well-prepared SSP ensures there are no compliance gaps and demonstrates readiness for potential assessments.
- **Applicable Evidence:** Generate and maintain evidence proving that the controls and restrictions defined in the SSP, network diagrams, asset inventory, and organizational policies, procedure, and practices are fully implemented. Be prepared to present this evidence if requested during a spot check or an expanded assessment (https://www.federalregister.gov/d/2024-22905/p-700).
- **Importance of Clear Documentation:** Comprehensive documentation is critical to the limited spot check process. Assessors depend on clear and accurate records to understand how CRMAs are categorized and managed. Incomplete or ambiguous documentation increases the likelihood of a "Not Met" result or the need for further assessment.
- **Risk of Deeper Dive:** Deficiencies or inconsistencies identified during a limited spot check can trigger an expanded evaluation, including evaluating the implementation of additional Level 2 controls on CRMAs. To mitigate this risk, proactively address any potential gaps in CRMA management before an assessment occurs.

Helpful Tip for FutureFeed Users

Use FutureFeed to map security controls directly to CRMA assets within your SSP. This feature makes it easy to demonstrate compliance, track implementation progress, and ensure assessors have clear documentation to validate your controls during the assessment.

By prioritizing thorough documentation, robust evidence generation, and proactive gap remediation, organizations can minimize the risks of compliance issues and ensure smoother assessments.

7. Conclusion

Effectively managing CRMAs is crucial for the protection of CUI confidentiality and compliance with NIST SP 800-171 Level 2 requirements under the CMMC. The CRMA designation was introduced to streamline assessments, but this flexibility relies heavily on the organization's ability to document and enforce robust policies, procedures, and practices that restrict CUI interaction.

By adhering to the recommendations outlined in this article, organizations can:

- Properly safeguard the confidentiality of CUI.
- Demonstrate compliance and readiness.
- Reduce interconnected system risk.
- Avoid failures, scoping issues, and expanded assessment.

Key Takeaways – be prepared to:

- Provide Organizational policies, procedures, and practices supporting CRMA designation.
- Provide an SSP that include method of implementation definitions for applicable Level 2 controls for CRMA assets.
- Provide diagrams and asset inventories that include CRMAs.
- Provide additional evidence.
- Conduct validation assessments on CRMAs.

Ultimately, managing CRMAs with diligence and precision safeguards not only CUI but also the organization's reputation and ability to meet its contractual obligations. By integrating this guidance into their risk management strategy, contractors can maintain a robust cybersecurity posture while benefiting from the reduced assessment burden intended for CRMAs.

Disclaimer

All references to CMMC in this document refer to the CMMC 2.0 final rule, released on October 15, 2024, by the DoD. All references to NIST SP 800-171 in this document refer to NIST SP 800-171 Revision 2, published by the National Institute of Standards and Technology in February 2020. The positions and opinions expressed in this paper are solely those of Rachel Leidy and do not reflect the official views of the DoD or the Cybersecurity Maturity Model Certification Accreditation Body (CyberAB). These interpretations are based on the latest CMMC rule and accompanying DoD commentary.

Please note that certain aspects of the CMMC rule remain ambiguous and lack comprehensive guidance. As such, interpretations or opinions may vary, and feedback or alternative perspectives are welcomed. This document is intended to foster discussion and collaboration, not to assert absolute conclusions.