GRC KNIGHT

WWW.GRCKNIGHT.COM

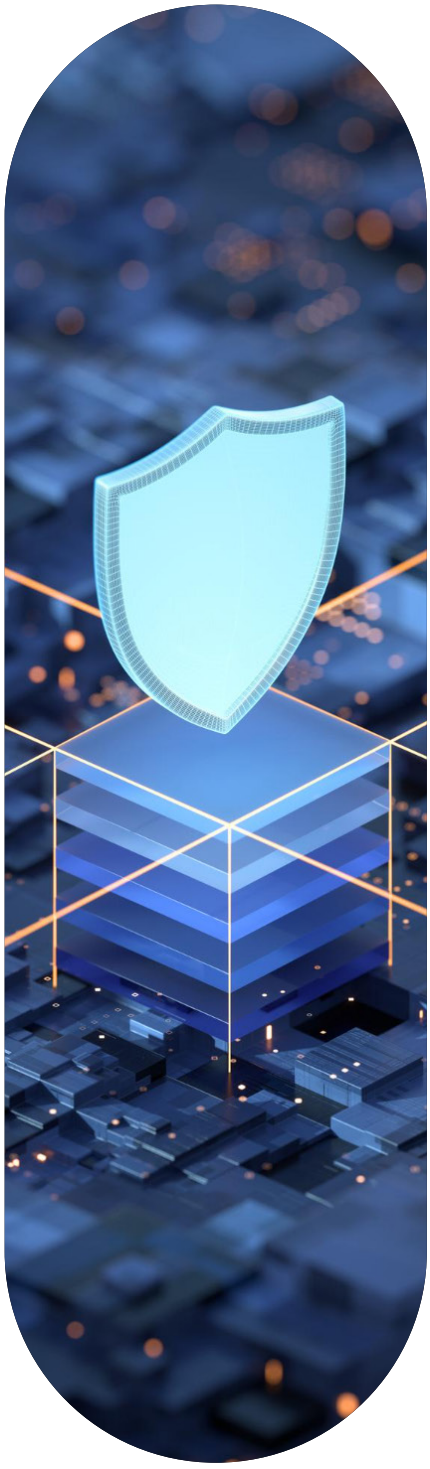
Survival Guide to **CMMC Compliance for Defense Subcontractors & SMBs**

Table of Contents

Introduction

Overview of CMMC

The Cybersecurity Maturity Model Certification (CMMC) was introduced in November 2021, aiming to enhance cybersecurity measures within the defense sector. This framework, developed by the Department of Defense (DoD), outlines a set of cybersecurity standards and practices, ensuring that contractors handling sensitive government data maintain a robust security posture.



Importance for Defense Sector Companies

For companies in the defense sector, particularly small to medium-sized businesses (SMBs), compliance with CMMC is not just a regulatory requirement but a necessity for securing, winning, and maintaining DoD contracts.

CMMC Implementation Timeline

Initial Announcement and Development

June 2019 - September 2020

The DoD first announced the CMMC program in June 2019, releasing version 1.0 of the CMMC model document in February 2020, and then published an interim rule in September 2020.

Restructuring to CMMC 2.0

November 2021

After receiving over 850 comments on the interim rule, the DoD reviewed and restructured the program into CMMC 2.0 in November 2021.

Recent Developments and Expectations

July 2022 - March 2023

The DoD expected to complete its documentation for the rulemaking process by July 2022 and to issue interim final rules by March 2023, but failed to meet their deadline.

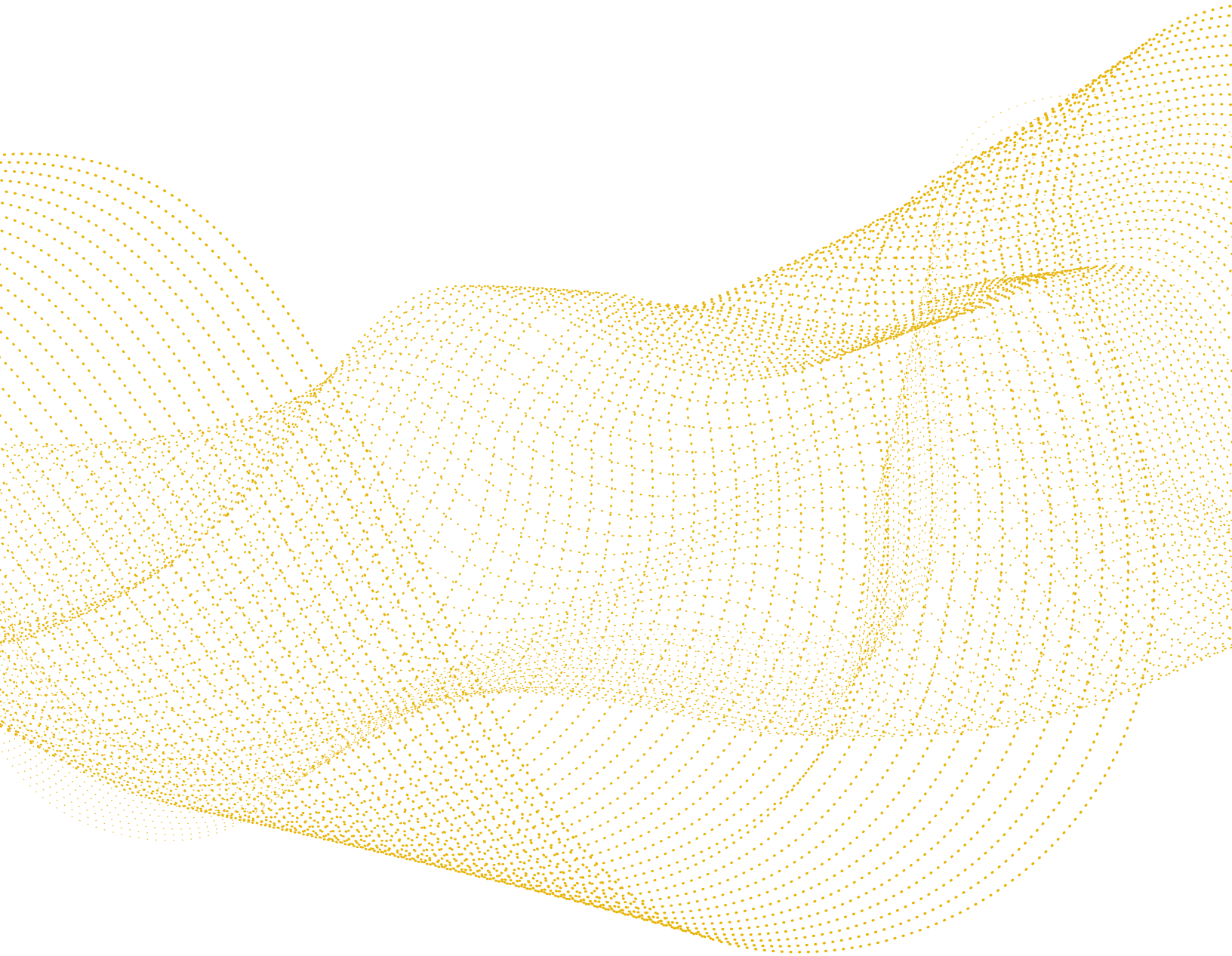
CMMC 2.0 Requirements in Solicitations

January 2024 and on

If the DoD sticks to this new timeline, CMMC requirements could begin appearing in solicitations as early as January 2024. This implementation will follow a phased approach, initially requiring all offerors to conduct a self-assessment and provide an affirmation of compliance. The subsequent phase, whose timing is yet to be determined, will require either self-assessments or third-party certifications depending on the type of CUI and the required certification level.

Preparation for CMMC

Companies should begin their compliance preparations immediately, given that it takes 12-18 months on average to become assessment-ready. This includes understanding the specific requirements of CMMC, implementing necessary cybersecurity controls, and conducting internal audits to ensure readiness for third-party certification.



Understanding **CMMC**

Origin of CMMC

CMMC has its roots in DFARS 7012 and NIST SP 800-171 Rev2, established to safeguard Controlled Unclassified Information (CUI) in non-federal systems. With evolving cyber threats, the Department of Defense (DoD) recognized the need for a more structured and comprehensive approach to cybersecurity, leading to the development of CMMC 1.0. In 2021, the DoD conducted an internal evaluation which incorporated over 850 comments on the model leading to a revised version which enhanced the program's structure and requirements.

CMMC 2.0: A Simplified Model

CMMC 2.0 MARKS A SIGNIFICANT SHIFT FROM ITS PREDECESSOR:

- **Compliance Level Reduction:** Streamlining from five levels to three enhances clarity and focus, and helps to minimize barriers to compliance while reducing costs.
- **Alignment with NIST Standards:** Now closely aligned with NIST SP 800-171 and SP 800-172, CMMC 2.0 ensures consistency with established cybersecurity best practices.
- **Practice Reduction for Level 2:** The number of practices required for Level 2 Certification has been reduced to 110.
- **Assessment Requirement Changes:** Modifications in assessment methodologies to reflect the revised structure.

Objectives of CMMC

The Cybersecurity Maturity Model Certification (CMMC) is designed to bolster the overall cybersecurity posture of the Defense Industrial Base (DIB). This is achieved through the implementation of standardized cybersecurity protocols and practices. In line with this overarching objective, CMMC aims to:

Elevate cybersecurity standards within the Defense Industrial Base (DIB):

By setting high cybersecurity benchmarks, CMMC ensures that all entities within the DIB are equipped to handle sophisticated cyber threats effectively.

Protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) from increasing cyber threats:

With the rise in cyber-attacks, safeguarding sensitive information becomes paramount. CMMC focuses on fortifying defenses against these evolving threats.

Ensure a uniform standard of cybersecurity readiness across all DoD contractors:

Uniformity in cybersecurity readiness ensures that all contractors are equally prepared to defend against cyber threats, thereby strengthening the security of the entire defense supply chain.

Understanding Controlled Unclassified Information (CUI) in CMMC

Controlled Unclassified Information (CUI) is a central aspect of CMMC, developed in response to the need for better protection of sensitive data within the Defense Industrial Base (DIB). Originally, defense contractors were required to self-certify compliance with NIST 800-171 to protect CUI, but this approach had limitations.

TYPES OF CUI:

CUI encompasses a broad range of information that is sensitive but not classified. Examples include:

- **Company Intellectual Property:** Trade secrets, patents, and proprietary information.
- **Sensitive Employee or Customer Data:** Personal details that could compromise privacy or security.
- **Health Records:** Protected health information that requires confidentiality.
- **Law Enforcement Records:** Information related to criminal investigations or legal proceedings.
- **Critical Infrastructure Information:** Details about key infrastructure that could impact national security if disclosed.
- **Export Control:** Information related to the export of sensitive goods or technology.
- **National Security Information:** Non-classified details relevant to national security interests.
- **International Agreements:** Documentation related to international treaties or agreements.
- **Dissemination Controls for CUI:** CUI can have specific dissemination controls indicating who can access and share the information. Examples include NOFORN (No Foreign Dissemination), FED ONLY (Federal Employees Only), and REL TO (Authorized for release to certain nationals only).

CUI BASIC VS. SPECIFIED:

- **CUI Basic:** Applies to general CUI where authorizing laws or policies don't provide specific protection guidelines.
- **CUI Specified:** Pertains to CUI requiring specific protections, like unique markings or enhanced physical safeguards.
- **Comparison with CDI (Covered Defense Information):** The DoD often uses CDI interchangeably with CUI. CDI includes CUI and requires contractors to safeguard it, report cyber incidents, and facilitate damage assessment.

PII AS CUI:

Personally Identifiable Information (PII), such as Social Security numbers or medical records, is protected as CUI under The Privacy Act.

CUI CATEGORIES IN DEFENSE:

The Defense Office of Inspector General (OIG) includes categories like Controlled Technical Information and DoD Critical Infrastructure Security Information as CUI.

CMMC REQUIREMENTS FOR CUI PROTECTION:

DIB contractors handling CUI must aim for CMMC Certified Level 3 compliance, which requires adherence to DoDI 8500.01 and 8510.01 instructions in all DoD systems.

PRACTICAL SCENARIO: CUI AND FEDERAL CONTRACT INFO (FCI) IN THE CONTEXT OF WEAPON MANUFACTURING

Let's consider a fictional company, "Orion Defense Systems," specializing in manufacturing advanced weaponry components. Orion has a subcontract with "Athena Aerospace," a prime contractor for the DoD.

EXAMPLES OF CUI:

- **Design Specifications:** Detailed blueprints of a new missile guidance system.
- **Test Results:** Data from performance tests of a prototype weapon.
- **Technical Memos:** Internal communications about the integration of new technologies in weapons.

EXAMPLES OF FCI:

- **Contract Agreements:** Details of the subcontract between Orion and Athena Aerospace.
- **Budget Reports:** Financial projections and expenditures related to the DoD project.

In this scenario, Orion must implement stringent security measures, like robust encryption protocols, to protect both CUI and FCI. Access to this sensitive information must be tightly controlled, ensuring that only authorized personnel within Orion and specific individuals at Athena Aerospace and the DoD can view or handle these documents. Any breach in these security protocols could compromise national security and the integrity of the defense manufacturing process.

CMMC Levels

Level 1 (Basic Cyber Hygiene):

As the foundational tier of the CMMC framework, Level 1 focuses on implementing basic cybersecurity practices. These are essential steps for any contractor in the Defense Industrial Base (DIB).

01 **Compliance Requirements:** At this level, compliance primarily involves self-assessment and reporting through the Supplier Performance Risk System (SPRS).

02 **Deadline:** Initially, Level 1 required annual self-assessments and affirmations. However, specific deadlines may vary as the Department of Defense (DoD) refines its expectations and phases in implementation.

Level 2 (Intermediate Cyber Hygiene):

Building on the foundational practices of Level 1, Level 2 shifts the focus towards establishing and documenting standardized cybersecurity processes. This level serves as a transitional phase towards more comprehensive cybersecurity practices.

01 **Compliance Requirements:** This level includes a mix of self-assessments for certain areas and third-party certifications for others.

02 **Deadline:** The third-party certifications required at this level are valid for three years, with an annual affirmation of compliance. Specific deadlines are set to align with the phased rollout of CMMC requirements in DoD contracts.

Level 3 (Good Cyber Hygiene):

Level 3 represents a significant step up, focusing on a comprehensive, managed cybersecurity program. This level is designed for entities that handle more sensitive information and face greater cybersecurity challenges.

01 **Compliance Requirements:** At this stage, a third-party certification becomes mandatory.

02 **Deadline:** Similar to Level 2, the certification is valid for three years, with an annual affirmation of compliance.

Levels 4 and 5 (Proactive and Advanced/Progressive):

These levels represent the pinnacle of cybersecurity maturity in the CMMC model. Level 4 is geared towards proactive cybersecurity measures, while Level 5 is the most rigorous, focusing on advanced and progressive cybersecurity practices.

01 **Compliance Requirements and Deadlines:** The detailed requirements and deadlines for these advanced levels are still under development, reflecting their complexity and the advanced nature of the cybersecurity measures involved.

NIST SP 800-171 vs 800-171A: **Understanding Compliance and Assessment**

Understanding NIST SP 800-171 and 800-171A

In the realm of cybersecurity for organizations handling Controlled Unclassified Information (CUI), adhering to the standards set by NIST SP 800-171 is crucial. This requirement is further reinforced by the NIST SP 800-171A, which provides specific guidelines for assessing compliance. Understanding the difference between these two documents is essential for organizations looking to ensure they meet the Department of Defense's cybersecurity standards.

EXAMPLE: ACCESS CONTROL - ENSURING AUTHORIZED ACCESS

NIST SP 800-171 (3.1.1) Requirement:

This section mandates that organizations limit system access exclusively to authorized users, processes acting on behalf of authorized users, or devices.

NIST SP 800-171A Assessment Objectives:

- **Verification**: Assess whether the organization restricts system access effectively to authorized entities only.
- **Implementation Assessment:** Evaluate the accuracy and completeness of implementation of these access controls.
- **Effectiveness Evaluation:** Determine the overall effectiveness of the access control measures in preventing unauthorized access.

EXAMPLE: INCIDENT RESPONSE - PREP FOR CYBERSECURITY INCIDENTS

NIST SP 800-171 (3.6.1) Requirement:

Organizations are required to have an established incident-handling capability that includes various aspects like preparation, detection, analysis, containment, recovery, and user response.

NIST SP 800-171A Assessment Objectives:

- **Capability Verification:** Confirm the existence of a comprehensive incident response system.
- **Process Assessment:** Ensure that incident response processes are properly implemented and are operational.
- **Effectiveness Evaluation:** Evaluate the readiness and effectiveness of the incident response team and the procedures in place.

Practical Implications and Compliance Strategies

Organizations aiming for compliance need to focus on both the establishment of the required security controls (as per NIST SP 800-171) and the ongoing assessment and improvement of these controls (as guided by NIST SP 800-171A). This dual focus ensures not only that the necessary security measures are in place but also that they are effective and up-to-date in an ever-evolving cyber threat landscape.

NIST SP 800-171 Parameters: Defining and Meeting Control Requirements

Understanding NIST SP 800-171 Parameters

NIST SP 800-171 provides a framework of security requirements designed to protect Controlled Unclassified Information (CUI) in non-federal systems and organizations. One of the key aspects of these requirements is the specification of parameters for certain controls. Parameters are customizable elements within a control that organizations need to define based on their specific environment and risk assessment. This customization allows the controls to be more effectively implemented and tailored to the unique needs and circumstances of each organization.

EXAMPLE: AUDIT AND ACCOUNTABILITY (3.3.1)

Control Requirement:

"Create and retain system audit logs and records to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity."

Parameters to Define:

- **Audit Log Content:** Organizations need to specify what information is to be captured in the audit logs. This might include user activities, system modifications, and access attempts.
- **Retention Period:** The organization must determine how long audit records will be retained, balancing the need for historical data with storage limitations and privacy concerns.
- **Monitoring Frequency:** Define how frequently the audit logs are to be reviewed. This could be daily, weekly, or based on specific triggers.
- **Reporting Procedures:** Establish parameters for how and when audit findings are reported, including escalation paths for potential security incidents.

Importance of Defining Parameters

Defining these parameters ensures that the control is applied in a manner that is both effective and aligned with the organization's cybersecurity strategy. The lack of well-defined parameters may lead to inadequate protection mechanisms or inefficient use of resources.

- Conduct a thorough risk assessment to understand their specific security needs.
- Involve stakeholders from different departments to gain a comprehensive view of operational requirements.
- Regularly review and update the parameters to adapt to changing threat landscapes and business needs.

Challenges and Solutions in Achieving CMMC Compliance

Common Compliance Challenges

Achieving CMMC compliance can be a daunting task for many organizations, with challenges ranging from understanding the scope of Controlled Unclassified Information (CUI) to ensuring secure configurations in technical systems. Below are a couple of scenarios that we at GRC Knight see quite often (for confidentiality purposes the use cases below have been anonymized and modified).

Challenges with Understanding CUI Scope and Boundaries: **A Case Study with SkyTech and Azure Information Protection**

UNDERSTANDING THE SCOPE, FLOW, AND BOUNDARY OF CUI AT SKYTECH

SkyTech, an aerospace parts manufacturer, was confronted with the intricate task of defining and managing Controlled Unclassified Information (CUI) within their complex systems. The challenge was not just in identifying CUI but also in understanding its flow and establishing necessary boundary controls, a critical requirement for CMMC compliance.

THE SOLUTION: CUI DATA DISCOVERY WITH MICROSOFT PURVIEW INFORMATION PROTECTION

To navigate this challenge, SkyTech enlisted the expertise of GRC Knight. This collaboration led to the deployment of a tailored solution using Microsoft Purview Information Protection, specifically configured to meet SkyTech's unique requirements.

01 **Comprehensive Data Discovery:** First, a thorough data discovery process was initiated. Utilizing Microsoft Purview, the team identified all instances of CUI within SkyTech's operational framework.

02 **Strategic Utilization of Microsoft Purview Capabilities:** GRC Knight then leveraged Purview's advanced data discovery tools and techniques. Key features such as sensitive information types, trainable classifiers, and data classification tools were employed to efficiently locate, categorize, and classify CUI data.

03 **Maintaining an Actionable Inventory:** An up-to-date inventory of CUI data types and their locations was maintained, utilizing the full capabilities of Microsoft Purview's data inventory functionalities.

04 **Protection Measures for CUI Data:** GRC Knight then implemented comprehensive data protection measures, which included encryption, access restrictions, and visual markings using Azure Information Protection's suite of tools like sensitivity labels, Double Key Encryption, and SharePoint Information Rights Management.

CONCLUSION AND IMPACT

With the strategic involvement of a CMMC expert at GRC Knight, SkyTech successfully overcame the challenge of CUI management. The bespoke solution not only ensured compliance with CMMC requirements but also significantly bolstered SkyTech's cybersecurity defenses. This case study exemplifies the effective synergy of expert guidance and advanced technological solutions in achieving CMMC compliance.

Implementing Effective Identity and Access Management with JumpCloud: **A CyberSecure Case Study**

THE CHALLENGE OF MANAGING ACCESS AND PERMISSIONS AT CYBERSECURE

CyberSecure, a dynamic cybersecurity solutions provider, encountered significant challenges in managing access controls within its growing organization. The complexity of their projects and the expansion of their team necessitated a robust solution to efficiently manage user access while ensuring data security.

THE SOLUTION: DEPLOYING JUMPCLOUD FOR ENHANCED SECURITY AND COMPLIANCE

To address these challenges, CyberSecure, in collaboration with GRC Knight, chose to deploy JumpCloud's open directory platform. This decision was pivotal in transforming their approach to identity and access management (IAM).

01 **Centralized Identity Management:** JumpCloud provided a unified platform for managing all user identities and their access rights. This "single pane of glass" approach significantly simplified the administration of user permissions.

02 **Federated Identities for Improved Security:** By federating identities, JumpCloud reduced the potential attack surface, enhancing overall security. This setup also enabled CyberSecure to act swiftly in the event of a security breach, thanks to centralized controls.

03 **Access Control Based on Least Privilege Principle:** JumpCloud's IAM system enforced the principle of least privilege, granting users only the access necessary for their roles. This approach minimized the risk associated with compromised credentials.

04 **Enhanced Security Measures:** The integration of multi-factor authentication (MFA) and single sign-on (SSO) significantly bolstered CyberSecure's defenses against credential theft and unauthorized access.

05 **Compliance with CMMC Domains:** The implementation of JumpCloud helped CyberSecure achieve compliance in multiple CMMC domains, including Access Control, Identification and Authentication, Incident Response, and more.

CONCLUSION AND IMPACT

The deployment of JumpCloud at CyberSecure, guided by the expertise of GRC Knight, not only resolved the immediate access control challenges but also aligned the company with CMMC compliance requirements. This strategic move enhanced CyberSecure's security infrastructure and positioned them as a compliant, secure, and efficient organization in the cybersecurity sector.

Secure Configuration Challenge and Solution: **DataSafe's Journey with GRC Knight and SteelCloud**

THE CONFIGURATION CHALLENGE AT DATASAFE

DataSafe, a data analytics SaaS company, faced a daunting task: securely configuring their systems to balance operational efficiency with stringent CMMC compliance requirements. Operating in an AWS environment with multiple Linux instances, the technical challenge was to ensure that their configurations met the rigorous standards set by Security Technical Implementation Guides (STIGs) without compromising their system performance or agility.

THE SOLUTION: AN INTERVENTION WITH STEELCLOUD

To tackle this complex issue, experts from GRC Knight administered and configured SteelCloud's ConfigOS, a powerful solution designed to streamline compliance with STIGs and CIS benchmarks.

01 **ConfigOS Implementation:** GRC Knight first implemented SteelCloud ConfigOS within DataSafe's AWS environment. This software provided an automated approach to manage compliance against STIGs for Linux instances.

02 **Non-Compliance Identification:** Utilizing ConfigOS, the specialist conducted an initial assessment to identify areas of non-compliance against the STIGs. This assessment was crucial in pinpointing specific configuration issues that needed attention.

03 **Testing Before Remediation:** Before deploying any configuration policies, DataSafe was guided through a thorough testing process, ensuring that the proposed changes would not adversely affect system performance or functionality.

04 **Config Policy Deployment:** Upon successful testing, ConfigOS policy containers were deployed that were tailored to DataSafe's specific environment. These policies enforced secure configurations while maintaining the necessary operational efficiency.

05 **Continuous Monitoring and Management:** The solution also included a continuous monitoring strategy, leveraging ConfigOS's capabilities to ensure that configurations remained secure and compliant over time.

CONCLUSION AND IMPACT

The deployment of SteelCloud ConfigOS enabled DataSafe to meet their secure configuration challenges head-on. This strategic move not only brought them into compliance with CMMC requirements but also enhanced their overall cybersecurity posture. DataSafe can now confidently assure their clients of the security and integrity of their data analytics services, thanks to a well-configured and compliant system environment.

GRC Knight's CMMC Implementation Project Plan

In the rapidly evolving landscape of cybersecurity, meeting the standards set by the Cybersecurity Maturity Model Certification (CMMC) is crucial for organizations within the Defense Industrial Base (DIB). To navigate this complex terrain, GRC Knight has developed a comprehensive implementation project plan to guide organizations through every aspect of CMMC compliance in a structured and efficient manner.

MILESTONE 1:

Data Management and Scope Definition

Objective: To precisely identify and manage Controlled Unclassified Information (CUI) and other sensitive data, and to define the extent of its flow within the organization.

KEY STEPS:

- Collaboratively identify and classify types of CUI and sensitive data.
- Develop Data Flow Diagrams (DFDs) to understand how CUI moves through the organization.
- Conduct an inventory of IT assets that interact with CUI, establishing clear boundaries for data management.

MILESTONE 2:

Security Documentation and Architecture

Objective: To establish robust security documentation and architecture that aligns with CMMC requirements.

KEY STEPS:

- Initiate and maintain a comprehensive System Security Plan (SSP) and Plan of Action & Milestones (POA&M).
- Analyze and design a secure network architecture, ensuring resilience against cyber threats.
- Regularly update and control access to security documents, reflecting changes in the security architecture.

MILESTONE 3:

Resource Allocation and Access Management

Objective: To strategically allocate resources and manage access controls effectively.

KEY STEPS:

- Prioritize resources based on legal, contractual, and security obligations.
- Implement Role-Based Access Control (RBAC) and conduct regular access reviews.
- Deploy identity and access management software for streamlined access control.

MILESTONE 4:

Risk Management and Change Control

Objective: To establish comprehensive risk management and change control processes.

KEY STEPS:

- Develop systematic risk identification and assessment methodologies
- Formulate a change management protocol and establish a Change Control Board (CCB).
- Document and review changes, ensuring stability, security, and compliance.

MILESTONE 5:

Incident Response and Situational Awareness

Objective: To prepare for and efficiently respond to security incidents while maintaining comprehensive situational awareness.

KEY STEPS:

- Draft and train on an incident response plan, covering roles, responsibilities, and protocols.
- Implement advanced security monitoring tools for continuous situational awareness.
- Conduct simulated incidents to test and refine the organization's response capabilities.

MILESTONE 6:

Technical and Physical Security Measures

Objective: To enforce strong technical and physical security measures.

KEY STEPS:

- Establish and audit baseline security configurations.
- Implement and regularly update encryption and physical security controls.
- Regularly conduct maintenance and vulnerability assessments.

MILESTONE 4:

Training, Auditing, and Continuous Improvement

Objective: To cultivate a security-conscious organizational culture and ensure ongoing compliance through regular training and auditing.

KEY STEPS:

- Develop comprehensive security training programs and conduct regular awareness sessions.
- Establish an internal audit program to assess and ensure adherence to CMMC standards.
- Continuously review and enhance security measures and training content based on emerging threats and technologies.

Navigating CMMC Compliance with GRC Knight

Key Takeaways

In our comprehensive guide, we dove into the intricate world of CMMC compliance, highlighting the critical components that small to medium-sized businesses in the defense sector must navigate. The key areas covered include:

01 **Understanding CMMC:** Tracing its origins from DFARS 7012 and NIST SP 800-171 Rev2, we explored the evolution of CMMC and its pivotal role in safeguarding CUI within the DIB.

02 **CMMC Levels and Deadlines:** We outlined the various levels of CMMC compliance, each with its specific focus and requirements, emphasizing the importance of timely preparation and adherence to these standards.

03 **NIST SP 800-171 vs 800-171A:** By illustrating the differences and connections between these two critical documents, we provided clarity on the compliance and assessment processes.

04 **Practical Scenarios and Solutions:** Through detailed case studies, we demonstrated real-world applications of CMMC compliance strategies, showcasing the expertise of GRC Knight in guiding organizations through complex cybersecurity challenges.

Encouragement to Stay Proactive in Cybersecurity Efforts

The path to CMMC compliance is continuous and requires a proactive stance. We encourage companies to stay vigilant and forward-thinking in their cybersecurity efforts. Regularly updating security measures, conducting training and audits, and adapting to emerging threats are essential steps in maintaining a robust cybersecurity posture.

Complimentary CMMC Readiness Gap Assessment

To further assist your journey towards CMMC compliance, GRC Knight offers a complimentary CMMC Readiness Gap Assessment. Our team of experts will provide insights into your current compliance status and identify areas for improvement, helping you navigate the complexities of CMMC with confidence.

Contact us at here for your free assessment and embark on a path to secure and compliant operations.