Achieving CMMC Level 2 Compliance in a Cloud-Native Architecture

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Joseph Yeboah served as the Team Lead for the Mobius CMMC project. He is currently working at Mobius LLC as a System Administrator and is a graduate student at George Mason University pursuing a Master's degree in Cybersecurity Engineering. In his role as Team Lead, Joseph was responsible for organizing the overall project structure, supervising intern work, and ensuring all deliverables aligned with CMMC requirements. He created the central folder structure used by the team, including documentation, supporting evidence, and tracking folders. He also developed the evidence templates and the Excel tracking workbook used to document control implementation status and link supporting artifacts. Joseph assigned control families to interns, monitored progress throughout the project, and reviewed all intern submissions before final inclusion to ensure accuracy, consistency, and alignment with CMMC expectations. His role focused on coordination, oversight, and quality control to ensure individual contributions were properly integrated into a complete CMMC compliance effort. Joseph's professional goal is to continue growing in cybersecurity and transition into roles such as Information System Security Officer (ISSO), Cybersecurity Engineer, or other advanced cybersecurity positions.

Tobi Alaofin is a senior Computer Science student at George Mason University and is pursuing a Master's degree in Computer Science with a concentration in Cybersecurity. He has gained hands-on industry experience as a Cybersecurity Engineer Intern at Mobius Consulting LLC, where he supported CMMC-aligned security control implementation, validation, and audit readiness activities under NIST SP 800-171. He also has experience as a Software Engineer at Delexis Health Care, contributing to the development of software solutions in a regulated healthcare environment. Driven by a strong interest in cybersecurity and cloud security, he is focused on building a solid foundation across software engineering, identity and access management, endpoint security, and security monitoring, with the goal of contributing to secure and compliant systems in professional roles.

Robel Mengesha is a senior at George Mason University graduating with a bachelor's degree in Management Information Systems. He has gained practical industry experience as a cybersecurity intern at Mobius Consulting LLC, contributing to compliance audit and security policy implementations. In addition to his formal education, he has worked to improve his technical skills through CodePath's Intro to Cybersecurity and Intro to Software Engineering courses. He is driven by a strong interest in the

evolving cybersecurity landscape, focusing on building a comprehensive foundation across multiple domains. Looking ahead, he plans to leverage his versatile technical background to tackle diverse security challenges upon his graduation

Kyle Kim is a graduate student at George Mason University pursuing a Master's degree in Cybersecurity, having previously earned a Bachelor of Science in Cybersecurity. He has gained hands-on industry experience as a Cybersecurity Analyst, supporting vulnerability management, security control implementation, and compliance alignment within cloud-based environments. His work has included assessing systems against industry frameworks such as NIST SP 800-53, CMMC, and OWASP Top 10, as well as assisting with remediation planning, security documentation, and audit readiness efforts.
In addition to his professional experience, Kyle has developed and maintained multiple cybersecurity projects focused on SIEM deployment, intrusion detection systems, honeypots, and secure cloud-native architectures. He holds several CompTIA certifications, including Security+, Network+, Server+, and CySA+, and actively participates in capture-the-flag challenges and applied security labs to strengthen his technical skill set. With a strong interest in compliance, cloud security, and risk management, Kyle aims to contribute to building secure, compliant, and resilient systems in professional cybersecurity roles.

----- ***Industry Participant / Mentor*** -----

William Ogus
Solutions Architect
Mobius Consulting

Joseph Yeboah
System Administrator
Mobius Consulting

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

As cyber threats targeting the defense industrial base continue to grow in sophistication and frequency, the U.S. Department of Defense (DoD) has mandated the Cybersecurity Maturity Model Certification (CMMC) to ensure that contractors adequately protect Controlled Unclassified Information (CUI). This project focused on supporting Mobius Consulting LLC, a modern IT consulting firm, in its preparation for a CMMC Level 2 readiness effort.

CMMC Level 2 requires adherence to the 110 security requirements defined in NIST Special Publication 800-171 Revision 2, spanning critical domains such as Access Control, Incident Response, Audit and Accountability, and System and Information Integrity. The project involved evaluating the organization's existing security posture, mapping regulatory requirements to technical controls, and assisting with the implementation and validation of configurations aligned with these federal standards. Leveraging the Microsoft security ecosystem, the team worked to establish a compliant, auditable security baseline and to develop evidence artifacts suitable for a future third-party assessment.

Business Challenge

Although Microsoft Compliance Manager provides a structured roadmap for achieving CMMC Level 2, a major challenge emerged in determining the applicability of its standardized "Improvement Actions" to Mobius Consulting's cloud-native architecture. Many recommended controls were designed with hybrid or on-premises environments in mind, creating the risk of implementing unnecessary or redundant configurations that did not meaningfully improve security.

This challenge required careful analysis to distinguish between controls that were truly required for compliance and those that represented legacy assumptions. Additionally, the team encountered inconsistencies in vendor-provided guidance. In several cases, Compliance Manager referenced deprecated dashboards or broken documentation links, disrupting the chain of evidence expected during an audit. As a result, the team had to independently research modern, valid evidence sources to ensure documentation remained accurate and defensible.

The transition from theoretical compliance planning to active enforcement introduced further complexity. During policy deployment, isolated configuration conflicts were discovered where new CMMC-aligned requirements conflicted with existing security settings. Identifying and resolving these conflicts was critical to ensuring that security controls were not only documented, but also technically enforced across managed endpoints.

Activities Done to Address the Business Challenge

To address these challenges, the team conducted a detailed control-by-control analysis of NIST SP 800-171 requirements and their associated Microsoft Compliance Manager improvement actions. Each control was evaluated for relevance within the organization's cloud environment, and only applicable technical requirements were selected for implementation. Key activities included:

- Reviewing identity, endpoint, and logging configurations across Microsoft security platforms
- Assisting with the deployment and validation of CMMC-aligned security policies
- Verifying control enforcement through configuration review and system behavior
- Identifying audit-relevant artifacts such as logs, policy states, and compliance reports
- Replacing deprecated or invalid evidence references with modern, verifiable sources
- Troubleshooting and resolving configuration conflicts during policy enforcement

Throughout the process, emphasis was placed on ensuring traceability from requirement to implementation and from implementation to evidence.

Results & The Positive Impact

As a result of this project, Mobius Consulting LLC achieved a significantly improved CMMC readiness posture. Applicable NIST SP 800-171 controls were clearly mapped to enforceable technical configurations, and redundant or inapplicable requirements were excluded, improving both efficiency and clarity. The organization benefited from:

- Clearer understanding of CMMC requirements within a cloud-native environment
- An auditable security baseline aligned with CMMC Level 2 expectations
- Improved evidence quality and traceability for future third-party assessments
- Reduced risk of assessment delays caused by incomplete or invalid documentation

Additionally, resolving configuration conflicts ensured that documented controls accurately reflected the organization's real-world security posture.

Conclusion

This project demonstrated the importance of applying critical judgment when translating regulatory frameworks into technical enforcement. Compliance is not achieved solely through checklist completion, but through thoughtful interpretation, accurate implementation, and verifiable evidence. By supporting Mobius Consulting's CMMC readiness effort, the project reinforced how compliance engineering, cloud security, and audit preparation intersect in practice. The experience highlighted the necessity of aligning regulatory intent with operational reality, particularly in modern cloud environments.

PREP Student Reflection

Participating in this project provided valuable insight into how cybersecurity compliance is executed in real-world organizational settings. Beyond understanding regulatory requirements at a theoretical level, The CMMC team gained experience in evaluating technical relevance, validating enforcement, and identifying audit-quality evidence. This work strengthened our appreciation for compliance engineering as a discipline that blends security architecture, operational risk management, and documentation rigor. It also emphasized the importance of adaptability, as vendor tooling and guidance do not always align cleanly with evolving cloud infrastructures. Overall, the project enhanced our ability to approach cybersecurity challenges analytically while balancing regulatory expectations with practical implementation.