Building CMMC Compliant GCC High Environment From the Ground Up with Mobius

A Professional Readiness Experiential Program (PREP) Project Effort

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

Taylor Le is a student at George Mason University graduating with a bachelor's degree in Information Technology and a concentration in Cybersecurity.

Raheem Zikria is a student at George Mason University graduating with a bachelor's degree in Information Technology and a concentration in Cybersecurity.

Brian Kim is a student at George Mason University graduating with a bachelor's degree in Cybersecurity Engineering.

Jeffrey Sterns is a student at James Madison University graduating with a Bachelor's degree in Computer Information Systems, with a concentration in Information and Cybersecurity Management.

Robel Mengesha is a student at George Mason University graduating with a bachelor's degree in Business with a concentration in Management Information Systems.

Abdirahman Mohamed is a student at George Mason University studying Information Technology with a concentration in Cybersecurity and Cloud Computing.

Michael Martell is a student at Northern Virginia Community College transferring to George Mason University in the fall of 2026 to pursue a Bachelors of Applied Science in Cybersecurity.

----- ***Industry Participant / Mentor*** -----
Wills Ogus
Technology Solutions Architect
Mobius

Lashdeep Singh
Director of Operations
Mobius

----- ***Faculty Member*** -----
Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
Assistant Dean, Centers of Excellence
George Mason University's Costello College of Business

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

Introduction

Mobius Consulting LLC operates in a federal contracting environment where security, compliance, and trust are essential. As the company prepares for CMMC v2.0 Level 2, it needs a secure and well-documented cloud environment that can support the handling of sensitive government-related information. Microsoft 365 GCC High was selected as a key platform because it is designed for organizations with government security and compliance needs.

Through the PREP program, our student team was given the opportunity to support this effort by helping Mobius stand up and organize a GCC High tenant from the ground up. The project gave the team hands-on exposure to real cloud security and compliance work. It also required us to think beyond classroom definitions of cybersecurity and understand how security controls must actually be implemented, tested, documented, and maintained in a working organization.

The team's role was to support the development of a secure foundation across multiple Microsoft services. This included work in Entra ID, Intune, Purview, Sentinel, Defender, Conditional Access, endpoint management, data protection, alerting, and compliance evidence collection. While each area had its own technical focus, the project was treated as one shared effort because CMMC readiness depends on how all of these pieces work together. The final goal was not just to configure individual tools. The broader goal was to help Mobius create a cloud environment that is secure, manageable, and easier to explain during future compliance reviews.

Business Challenge

Mobius needed to move from general CMMC guidance to a practical implementation model inside Microsoft 365 GCC High. This created several challenges.

First, CMMC requirements are broad by design. They describe security outcomes that must be met, but they do not give a simple step-by-step configuration guide for every organization. Mobius needed to determine how each requirement applied to its own environment, users, data, and business processes.

Second, Microsoft 365 GCC High includes many different security and compliance tools. These tools are powerful, but they can also overlap. For example, Microsoft Purview may support data protection, DLP, labeling, and compliance evidence. Microsoft Entra ID may support authentication, access control, role management, and Conditional Access. Microsoft Intune may support device security, compliance enforcement, and mobile device management. The challenge was not only knowing which tool could help, but knowing how each tool should fit into the larger compliance picture.

Third, the environment needed to remain realistic for a small and highly technical organization. A control can be technically strong but still difficult to maintain if it creates too much administrative burden. The team had to consider whether the recommended settings, policies, and documentation could actually be sustained over time.

Fourth, Mobius needed evidence that could support future assessment preparation. In a compliance environment, it is not enough to say that a control exists. The organization must be able to show what was configured, why it was configured, how it was validated, and how it supports a specific compliance objective. This made documentation one of the most important parts of the project. Because of these challenges, the project became both a technical security effort and a compliance documentation effort. The team had to help Mobius make progress in both areas at the same time.

Project Approach

The student team approached the project by organizing the work into major security and compliance domains. Each team member focused on a specific area, but the team continued to coordinate across domains because many controls depended on one another.

The project approach included five major steps.

1. *Understanding the GCC High Environment*
   The team first needed to understand the purpose of the new Microsoft 365 GCC High tenant and how it related to Mobius' CMMC preparation. This included reviewing the major Microsoft services being used, understanding the general system boundary, and identifying where security controls would need to be implemented or documented.

2. *Reviewing CMMC-Aligned Guidance*
   The team reviewed CMMC-related expectations and Microsoft's recommended improvement actions. This helped identify which technical areas needed attention and how Microsoft tools could support specific security practices.

3. *Dividing Work by Product Area*
   The team divided responsibilities across major technical areas, including Microsoft Sentinel, Microsoft Defender, Microsoft Purview, Microsoft Intune, Microsoft Entra ID, Conditional Access, DLP, information protection, and cloud security. This allowed each team member to develop deeper knowledge in one area while still contributing to the overall compliance effort.

4. *Implementing and Validating Controls*
   The team helped configure, review, and validate security settings across the GCC High tenant. This included checking whether policies behaved as expected, whether alerts or restrictions worked correctly, and whether configurations supported the intended compliance goal.

5. *Documenting Evidence and Results*
   The team created written evidence and practical explanations that connected technical work back to CMMC objectives. This documentation was important because it helped turn configuration work into something that could be reviewed, maintained, and reused during future assessment preparation.

Activities Done to Address the Business Challenge

1. Identity and Access Management
The team supported identity and access management work within Microsoft Entra ID. This area focused on making sure users, roles, and access decisions were governed in a secure and consistent way. The work included reviewing authentication requirements, supporting multifactor authentication enforcement, examining privileged role assignments, and helping align access control settings with CMMC expectations. The team also looked at how user access should be limited based on business need, job role, and security risk. Identity was one of the most important areas of the project because it affects nearly every other part of the environment. If access control is weak, other protections become less effective. For that reason, the team treated Entra ID and Conditional Access as core parts of the GCC High security foundation.

2. Conditional Access
Conditional Access was used to help control when and how users can access Microsoft 365 resources. The team supported the design and review of access rules that could consider factors such as user identity, device compliance, authentication strength, and risk. This work helped connect identity security with endpoint management. For example, access decisions can be tied to whether a device is managed and compliant. This creates a stronger security model because users are not only required to sign in securely, but also to access resources from devices that meet the organization's security expectations. The team also considered how Conditional Access policies affect real users. A policy that is too weak may not meet security goals, but a policy that is too strict may block normal business activity. The team's work helped support a more balanced approach.

3. Microsoft Intune and Device Management
The team supported Microsoft Intune work related to endpoint and mobile device management. This included helping establish device compliance baselines for Windows, macOS, iOS, and Android devices. Device compliance policies focused on important security expectations such as encryption, operating system requirements, password settings, and managed device status. These policies help ensure that devices accessing company resources meet minimum security standards. The team also helped connect Intune compliance with Conditional Access so that device trust could become part of the access decision. This is important for CMMC readiness because unmanaged or noncompliant devices can create risk when accessing sensitive information. This work also helped Mobius move toward a more consistent device governance model. Instead of relying only on user behavior or manual review, Intune provides a way to apply and measure device requirements more consistently across the environment.

4. Microsoft Purview and Information Protection
The team supported Microsoft Purview work focused on protecting sensitive information across the GCC High tenant. This included sensitivity labels, label policies, encryption-related behavior, and information protection settings across services such as Exchange, SharePoint, OneDrive,

and Teams. Information protection was a major part of the project because CMMC Level 2 focuses heavily on protecting Controlled Unclassified Information. The team helped ensure that sensitive information could be identified, labeled, protected, and handled according to organizational expectations. The work also included reviewing how information protection settings aligned with the organization's previous environment and adapting those settings for GCC High. This was important because the goal was not only to create a secure environment, but also to maintain consistency where appropriate.

5. Data Loss Prevention

The team supported the configuration and validation of Microsoft Purview Data Loss Prevention policies. These policies help detect and prevent sensitive information from being shared or exposed in ways that could create compliance or security risk. DLP work included coverage across Exchange, SharePoint, OneDrive, and Teams. The team reviewed how policies could monitor sensitive content, trigger alerts, restrict certain actions, notify users, and help reduce the chance of unauthorized sharing. This work was especially important because CMMC readiness depends on more than storing information securely. The organization also needs to control how information moves, who can access it, and whether users are warned or blocked when a risky action occurs. The team also documented DLP configuration and validation steps so the organization could explain how these protections support specific compliance objectives.

6. Microsoft Sentinel and Monitoring

The team supported Microsoft Sentinel work related to security monitoring, alerting, and visibility. Sentinel helps collect and analyze security-related activity so that the organization can identify suspicious behavior and respond more effectively. The team contributed to monitoring use cases related to user activity, authentication, endpoint behavior, audit information, email security, and insider risk indicators. The goal was to help Mobius improve its ability to detect and review activity that may matter from a security or compliance standpoint. Monitoring was important because CMMC readiness is not only about preventing issues. It also requires the organization to notice security-relevant activity, review it, and maintain evidence that monitoring practices are in place. The team also helped create documentation explaining what monitoring capabilities were implemented, how they support compliance expectations, and how evidence could be reviewed later.

7. Microsoft Defender

The team supported Microsoft Defender-related work as part of the broader security foundation. Defender capabilities help protect users, devices, identities, and cloud services from security threats. The team reviewed how Defender tools could support endpoint protection, email security, threat detection, alert review, and security posture management. This work helped connect technical defense capabilities with CMMC expectations around monitoring, protection, and response readiness. Rather than treating Defender as one isolated tool, the team viewed it as part of a larger security ecosystem. Defender alerts, Intune device compliance, Entra ID identity controls, and Sentinel monitoring all work together to create a stronger picture of the environment's security posture.

8. Cloud Security and Configuration Governance
The team also supported cloud security and configuration governance work. This involved reviewing baseline settings, secure configuration expectations, and cloud service governance practices that help keep the GCC High tenant consistent and manageable. This area was important because CMMC readiness requires more than one-time setup. The organization needs repeatable practices for maintaining secure configurations over time. The team helped document these practices and connect them to the organization's broader compliance foundation. Cloud security work also helped reduce ambiguity around shared responsibility. Microsoft provides the cloud platform, but Mobius is still responsible for configuring its tenant, managing users, protecting data, and maintaining evidence. The team helped clarify how tenant-level settings and operational practices support those responsibilities.

9. Compliance Manager and Evidence Collection
The team used Microsoft Compliance Manager and related documentation processes to connect implementation work with CMMC-aligned improvement actions. This was one of the most important parts of the project because compliance work must be provable. For each relevant area, the team helped document what was done, what was reviewed, how the control was validated, and what evidence could support future assessment work. The documentation was written to be practical and understandable. The goal was to make it easier for Mobius to maintain the evidence after the project ended and to support future System Security Plan updates.

Results & The Positive Impact
The project helped Mobius move closer to CMMC Level 2 readiness by creating a stronger technical and documentation foundation inside Microsoft 365 GCC High.

1. *Stronger Security Foundation:* The team helped support controls across identity, access, devices, data protection, monitoring, and cloud governance. These areas are central to protecting sensitive information and reducing risk in a cloud environment.

2. *Clearer Compliance Alignment:* The project helped connect CMMC expectations to Microsoft GCC High capabilities. This gave Mobius a clearer understanding of how its tools and configurations support future compliance goals.

3. *Improved Evidence Collection:* The team created documentation that explains implementation steps, validation activities, and evidence locations. This helps make the environment easier to review and maintain.

4. *More Sustainable Processes:* The team focused on practical implementation rather than overcomplicated controls. This helped create a foundation that Mobius can continue to improve after the PREP engagement.

5. *Better Cross-Domain Coordination:* The project improved alignment across security areas that often overlap, such as identity, endpoint management, DLP, monitoring, and access control.

6. *Future Assessment Support:* The work created a stronger starting point for future System Security Plan updates, internal reviews, and third-party assessment preparation.

Conclusion

Through this PREP engagement, the student team helped Mobius Consulting LLC build a stronger Microsoft 365 GCC High foundation for CMMC v2.0 Level 2 readiness. The team supported technical implementation, validation, documentation, and evidence collection across several major security and compliance areas.

The work helped translate broad CMMC requirements into practical cloud security actions. It also helped connect Microsoft GCC High capabilities to the organization's real operating environment. By focusing on identity, endpoint management, information protection, DLP, monitoring, Defender, Sentinel, cloud governance, and documentation, the team helped create a more complete and sustainable compliance foundation.

Most importantly, the project showed that CMMC readiness depends on more than enabling security features. It requires a coordinated approach where technical controls, business processes, documentation, and evidence all support one another. The student team's work helped Mobius take a meaningful step toward that goal while gaining real experience in cloud security, compliance, and federal contracting environments.

PREP Student Reflection

One of the most valuable parts of this project was the opportunity to help build a Microsoft 365 GCC High environment from the ground up instead of simply maintaining an existing one. Most students and even many professionals only gain experience working within environments that have already been established, where policies, architectures, and operational processes are already in place. Through this engagement, our team had the rare opportunity to be involved in the early stages of designing, organizing, and implementing a GCC High tenant intended to support real CMMC Level 2 preparation efforts.

What made the experience especially meaningful was the level of ownership given to the student team. Rather than only observing or assisting with isolated tasks, each student was trusted to lead a major product or security area within the environment. Team members took responsibility for areas such as Microsoft Sentinel, Microsoft Defender, Microsoft Purview, Data Loss Prevention, Microsoft Intune, Conditional Access, cloud security governance, identity and access management, and compliance documentation. This created an experience that felt much closer to a real security engineering and compliance team than a traditional internship assignment.

The project also demonstrated how interconnected modern cloud security environments really are. Even though each student had a primary focus area, no one worked in isolation. Decisions involving Conditional Access affected device compliance. Information protection policies impacted collaboration workflows and user access. Monitoring and alerting configurations influenced incident response readiness and evidence collection. Because of this, the team constantly collaborated to ensure configurations, documentation, and security goals stayed aligned across the tenant.

Another major takeaway was learning how compliance frameworks like CMMC function in practice. Before this experience, many of us understood compliance primarily from an academic perspective through diagrams, control families, and written requirements. This project showed us how much interpretation, coordination, and operational planning is required to actually implement those expectations inside a working environment. We learned that compliance is not just about enabling settings. It requires documentation, validation, repeatable processes, evidence collection, and long-term maintainability.

Working inside a live GCC High environment also gave the team exposure to challenges that are difficult to replicate in a classroom setting. We had to think about how security controls would impact real users, how policies could realistically be maintained by the organization, and how implementation decisions would later be explained during future assessments or audits. The project required balancing technical security goals with usability, sustainability, and business operations.

Overall, this engagement provided a level of hands-on cloud security and compliance experience that is uncommon for students entering the industry. Being able to say we helped stand up and organize a GCC High environment from the beginning, while leading individual product areas and contributing to a broader CMMC readiness effort, gave us experience that extends far beyond simply maintaining preexisting systems. It strengthened both our technical understanding and our ability to work collaboratively in a real-world security and compliance environment.