



## Microsoft 365 GCC High Rapid Deployment

### HIGHLIGHTS

- **Rapidly deploy Microsoft 365 for CMMC 2.0 Compliance:** Set up a fully configured tenant with built-in compliance and security settings to meet regulatory requirements.
- **Strengthen Identity and Access Security:** Verify user access, implement MFA, and establish governance to prevent unauthorized access and secure accounts.
- **Protect Sensitive Data and Detect Threats:** Leverage advanced endpoint protection, threat detection, data loss prevention, and labeling policies to shield sensitive information and mitigate risks.

### ABOUT DAYMARK

Daymark Solutions excels in creating sophisticated technology solutions, specializing in addressing complex business challenges through expertly designed systems. Their highly skilled architects are adept at crafting well-architected solutions that seamlessly integrate cloud and data center technologies. By combining these technologies, they create robust, scalable and secure systems tailored to meet their clients' unique needs.

*Deploy Microsoft 365 GCC High services in days, not weeks, while leveraging Daymark's enhanced security baseline.*

### OVERVIEW

Organizations in regulated sectors, like defense and government contracting, are under growing pressure to protect sensitive data and comply with stringent standards like Cybersecurity Maturity Model Certification (CMMC 2.0). Compliance with these standards is increasingly essential for contract eligibility as non-compliance can lead to immediate disqualification from government contracts, resulting in lost revenue and competitive disadvantages. Additionally, financial and legal risks from non-compliance are substantial. Failing to meet federal mandates can lead to fines, legal consequences, and significant reputational harm, potentially eroding client trust and market positioning.

Daymark's GCC High - Rapid Tenant Deployment offers a secure and expertly configured Microsoft 365 GCC High environment designed for CMMC 2.0 requirements and positioning organizations for continued eligibility in highly regulated markets. Daymark's experienced consultants manage each step of the deployment, aligning with regulatory and security standards to ensure that the solution is tailored to the specific compliance needs of the organization, from data protection to auditing controls. This customized deployment minimizes the time and complexity involved, allowing organizations to advance their compliance journey swiftly and confidently.

In short, Daymark's solution facilitates rapid tenant deployment with CMMC 2.0-focused configurations and enhances the organization's ability to independently maintain a secure Microsoft 365 environment. This leads to reduced risk, increased operational resilience, and sustained contract eligibility in regulated markets.

## OUTCOMES

Daymark consultants will:

- **Establish a Secure Microsoft 365 Environment:** Configure Microsoft 365 GCC High with CMMC 2.0 controls to protect sensitive government data and ensure regulatory compliance.
- **Enable Secure and Verified IT Access:** Implement identity governance and access controls to safeguard the tenant and reduce risks.
- **Maintain Compliance:** Manage the tenant effectively with detailed documentation of configurations, security settings, and compliance workflows, ensuring continued alignment with CMMC 2.0 standards while working toward CMMC 2.0 compliance.

## AGENDA

### Workstream 1: Initial Configuration and Core Security Setup

- **Objective:** Configure foundational security policies in the Microsoft 365 GCC High tenant to align with CMMC 2.0 requirements.
- **Activities:**
  - Set up Microsoft 365 GCC High tenant with baseline security.
  - Configure Entra ID for identity management and implement Privileged Identity Management (PIM) for controlled role-based access.
  - Enforce multi-factor authentication.
  - Configure licenses with group-based licensing.
  - Establish secure access policies with conditional access.
  - Set up anti-spam, anti-malware, anti-phishing, Safe Attachments, and Safe Links using Defender for Office 365.

### Workstream 2: Endpoint Security, Information Protection, and Documentation

- **Objective:** Implement endpoint protection, information protection policies, and create documentation for IT management and compliance readiness.
- **Activities:**
  - Deploy Next-Gen Protection, Endpoint Detection and Response (EDR), and Vulnerability Management.
  - Implement security baselines to ensure device compliance.
  - Configure labeling for sensitive data with Purview Information Protection.
  - Implement Data Loss Prevention (DLP) policies across Microsoft 365 services.
  - Set up device registration with Intune, compliance policies, and conditional access.
  - Compile Entra ID, Conditional Access, Defender policies, PIM, and DLP documentation.

Learn more about Daymark Solutions, visit [www.daymarksi.com](http://www.daymarksi.com)

**Daymark Solutions, Inc.**  
131 Middlesex Turnpike  
Burlington, Massachusetts 01803

+1.781.359.3000  
info@daymarksi.com  
www.daymarksi.com

