



How will CMMC assist your business?

About Eide Bailly:

At Eide Bailly, we're more than just consultants; we're innovators and strategic partners dedicated to maximizing the potential of Microsoft to help support your CMMC journey. Our depth and breadth of technology experts, combined with deep industry knowledge in healthcare, manufacturing and distribution, financial institutions, non-profits, and public sector means that you will get expert guidance on responsible CMMC usage that brings you immediate business value.

What we offer

To support readiness for CMMC Level 2 certification, this service delivers a comprehensive set of preparation activities addressing both technical and programmatic requirements. It includes the design and deployment of a secure enclave on compliant infrastructure (such as Microsoft Azure Government or GCC High) to protect Controlled Unclassified Information (CUI), along with full implementation of technical controls outlined in a CMMC Shared Responsibility Matrix.

In parallel, the service provides tailored documentation essential for certification, including a System Security Plan (SSP), cybersecurity policies and procedures, and secure configuration baselines. These materials are customized to reflect the organization's environment and structured to meet assessor expectations. Together, the technical and documentation efforts help ensure the organization is fully prepared for a successful CMMC Level 2 assessment, with infrastructure and governance aligned to NIST SP 800-171.

Eide Bailly, LLP

www.eidebailly.com/microsoft | d365bcsupport@eidebailly.com | 844-476-8957

[See our offer on the Microsoft Commercial Marketplace](#)

What our customers are saying

"Eide Bailly really raises the level of your technology and what you can do in your business."

– Robb Swanson, Operating Partner,
Zorbaz

Why Microsoft CMMC?

What's Included

- Secure enclave deployment on compliant infrastructure (e.g., Azure Government or GCC High) to protect CUI.
- Implementation of technical controls from the CMMC Shared Responsibility Matrix, including network segmentation, access controls, and endpoint hardening.
- Creation of a System Security Plan (SSP)
- Tailored cybersecurity policies and secure configuration baselines aligned to NIST SP 800-171.

Why CMMC Launchpad Services?

- Achieve CMMC Level 2 readiness through a structured approach.
- Deploy secure infrastructure such as Azure Government or GCC High.
- Implement critical cybersecurity controls.
- Receive tailored documentation.

