

A Future-Proof Approach to CMMC Level 2:

How a Hybrid CUI Environment Reduced Scope and Accelerated Readiness

NCAB Group (NCAB) produces printed circuit boards (PCBs) for defense organizations worldwide. Headquartered in Sweden but with U.S. operational divisions, the company's Department of Defense (DoD) contracts involve maintaining and securing Controlled Unclassified Information (CUI), requiring it to hold CMMC Level 2 certification. A key certification criterion was operating a secure, scalable cloud environment aligned to U.S. compliance standards.

Working in partnership with Redspin, the company implemented a hybrid cloud model that includes a secure, isolated GCC-High GovCloud environment for handling its US-sensitive government business data. Redspin supported configuration and security reviews across NCAB's cloud, including Managed Azure and Managed Microsoft 365 implementations. With Redspin's help, NCAB successfully completed a CMMC Level 2 Assessment, a major milestone in the company's journey.

The Level 2 Certification Decision

Why did NCAB go after CMMC Level 2?

CMMC Level 2 became important as the DoD began formally validating cybersecurity requirements that had long existed for Defense Industrial Base (DIB) contractors, particularly regarding the protection of CUI. While these expectations were already established through DFARS and alignment with NIST SP 800-171, CMMC introduces a structured, third-party assessment to verify implementation. We pursued CMMC Level 2 to ensure we can continue supporting customers with immediate requirements for secure, compliant PCB sourcing, while also preparing for those who will soon be subject to these requirements through contract flow-downs.

We are proud to be among the first in the PCB industry to achieve CMMC Level 2 certification.

When NCAB first began exploring CMMC, what was your understanding of the requirements and your organization's readiness at that time?

NCAB Group's IT team was very familiar with the National Institute of Standards and Technology (NIST) guidance. We already had a level of these controls in place in our legacy International Traffic in Arms Regulations (ITAR)-regulated environment. That environment was also hosted in Azure Government Cloud. Still, our team lacked deep familiarity with the best practices and tools needed to support complete coverage of the required controls and make them manageable.

What was NCAB's primary reason for leveraging Redspin's managed cloud services?

The primary driver was to reduce the scope of systems that fall under our CMMC Level 2 compliance requirements so we could accelerate and simplify our readiness for assessment. We were looking for expert support in implementing and operationalizing CMMC requirements along with a pre-hardened architecture aligned to the NIST 800-171 standard for protecting CUI. We were also interested in reducing our assessment burden and internal maintenance efforts, ideally through the use of a managed service with dedicated expertise in these areas.

Starting on the Assessment Path

What were your biggest concerns or unknowns early in the CMMC process?

Early in our CMMC journey, our biggest challenges centered on making the right architectural decisions for a compliant environment. We also faced uncertainty around procurement standards and the overall complexity of meeting CMMC Level 2, especially in a distributed, international organization. These unknowns shaped our decisions to pursue a well-structured, U.S.-only cloud architecture and to lean on specialized partners to accelerate our readiness.

With so many options, what considerations went into this decision? Why GCC High, why a hybrid model, long-term vs. short-term planning?

When evaluating options for a CMMC-aligned environment, several factors shaped our direction. First, the need to protect CUI within a fully U.S.-based infrastructure led us to Microsoft GCC High. The environment offers the compliance assurances, data residency guarantees, and FedRAMP High-aligned controls required for long-term CMMC Level 2 needs.

At the same time, we recognized that re-engineering the entire global IT landscape was neither practical nor aligned with our business priorities. This drove the decision to adopt a hybrid model, allowing us to isolate CUI into a secure, U.S.-only enclave while keeping our global systems and processes unchanged.

Balancing short-term readiness with long-term scalability was also central to the decision. In the short term, we needed a solution that could accelerate CMMC compliance without disrupting operations

In the long term, we needed a platform that could evolve with maturing requirements, support future DoD programs, and avoid costly re-architecture later. GCC High, paired with a hybrid enclave model, met all of these needs—delivering a compliant, contained, and future-proof approach.

What gave NCAB confidence that Redspin was the right partner for CMMC?

We gained confidence in Redspin based on their deep, proven expertise and long-standing participation in the CMMC ecosystem. They were able to guide organizations through both the technical and operational aspects of CMMC Level 2 and ongoing compliance maintenance once we had achieved CMMC Level 2. Redspin's experience as a C3PAO and team of technical experts that focused on the best solution for us and our complex business assured us that they understood the full assessment lifecycle, not just the technology, but what assessors actually looked for.

Equally important, Redspin offered a clear, practical architecture path for a U.S.-only, CUI-compliant environment built on Microsoft Azure Government. Their managed-enclave approach aligned with our hybrid strategy, reduced our internal CUI scope, and provided a faster, more predictable path to readiness. Redspin also demonstrated strong operational maturity, transparent communication, and a track record of helping companies avoid costly missteps during CMMC planning.

Together, these factors gave us confidence that Redspin could deliver a compliant, sustainable, and strategically sound CMMC solution.

As one might expect, we had a lot of questions about the requirements and the process. To support this, Redspin established weekly working sessions that created a consistent cadence and clear structure for the engagement. These sessions created a structured rhythm that kept the project moving forward and ensured every technical and compliance decision was fully understood before implementation. The structured weekly meetings allowed us to work through complex CMMC requirements in manageable steps, gain clarity quickly, and adjust plans as new details emerged. The collaborative environment—where both teams openly shared challenges, options, and best practices—built a strong sense of partnership and trust. As a result, the project maintained momentum, avoided rework, and delivered an aligned and well-designed solution that we feel provides the flexibility to meet our current CMMC compliance needs and our longer-term business strategy.

Certification Results & Impact

How would you describe Redspin's role in guiding NCAB from early in the program through successful Level 2 assessment readiness?

Redspin guided NCAB from initial uncertainty to full readiness for a CMMC Level 2 assessment. Their support spanned both the technical and compliance domains, beginning with architecture design and extending through detailed documentation and pre-assessment preparation. Redspin helped NCAB evaluate options and ultimately define a secure, U.S.-only Azure Government environment that aligned with CMMC requirements and manageability over time. They provided hands-on guidance in configuring the environment, reviewing controls, and validating that security settings met NIST 800-171 and CMMC expectations.

On the compliance side, Redspin supported the development and refinement of key documentation—including policies, procedures, and the System Security Plan—and ensured each element tied back to technical evidence. Regular working sessions allowed NCAB to confirm interpretations, resolve uncertainties, and make informed decisions quickly. As the program progressed, Redspin conducted thorough configuration reviews and walked the team through pre-assessment exercises, helping NCAB understand what assessors would expect and where additional hardening or clarification was needed. Through this structured and collaborative approach, Redspin provided clear guidance, reduced complexity, and helped ensure NCAB was positioned confidently for its Level 2 assessment.

What did the successful completion of the CMMC Level 2 assessment mean for NCAB?

Achieving a perfect score of 110/110 and successfully passing the CMMC Level 2 C3PAO assessment were major milestones for us. This validated that our U.S. operations meet the full set of NIST 800-171 security requirements, and that our technical, procedural, and governance controls operate at a high level of maturity.

Beyond the certification itself, the outcome is having a significant business impact. It positions us as a trusted and fully compliant supplier within the U.S. defense industrial base at a time when CMMC requirements are becoming integral to DoD contracting. This strengthens our competitive position, protects key customer relationships, and opens the door to new opportunities that require a verified CMMC posture.

The successful assessment also reinforces the long-term value of our hybrid GCC High and enclave-based architecture. By building a future-proof environment early, we've reduced risk, minimized our assessment burden, and established a secure, scalable foundation for ongoing CUI work. Overall, the achievement demonstrates NCAB's commitment to meeting the highest cybersecurity standards and delivering reliable, compliant manufacturing services to U.S. defense partners.

What is the value of managed cloud services going forward?

Now that NCAB has achieved CMMC Level 2 certification with a perfect score, the value of our managed cloud services shifts from achieving compliance to staying secure, scalable, and aligned with long-term U.S. defense business goals. The enclave and GCC High environment provide a stable foundation that reduces operational risk, simplifies ongoing compliance obligations, and enables us to confidently support future DoD programs without re-architecting our systems.

Operationally, leveraging the fully managed service model means NCAB continues to benefit from expert monitoring, configuration validation, and continuous improvement—all essential for maintaining a mature CUI environment in Azure Government.



Who is NCAB Group?

We are a leading supplier of printed circuit boards (PCBs) for demanding customers, delivered on time with zero defects, produced sustainably at the lowest total cost. Since our founding in 1993, we have grown to a worldwide enterprise with customers in 45 markets supported by 660 local specialists globally.

Defense is naturally a key industry sector for us. Our area of expertise focuses on high-reliability PCBs where failure is not an option. The modern defense industry has increased demands for secure, ruggedized, and precise technologies to support a range of applications—from fighter jets and air defense to naval propulsion and surface radar to satellite communications equipment and more. We are honored to support our customers within the sector with the peace of mind that their project’s data is handled in full compliance with the utmost care, vigilance, and comprehensive processes in place for optimal risk mitigation.

As CMMC evolves and requirements tighten, we have gained a partnership with Redspin and a solution that will be cost-effective and flexible to future changes, minimizing disruption to our broader global IT landscape.

From a business standpoint, the certified and fully managed environment strengthens NCAB’s position in the U.S. defense industrial base. It supports customer trust, enhances competitive differentiation, and enables us to pursue opportunities that require validated CMMC compliance. Most importantly, the long-term model allows our U.S. operations to scale securely while enabling the global NCAB organization to remain agile and focused on its core manufacturing mission.

What’s the best way for international companies to prepare for CMMC Level 2?

Pursuing CMMC Level 2 can feel overwhelming at first—especially when balancing U.S. compliance requirements with an international workforce and infrastructure. The key is to approach it with clarity and a long-term strategy. Start by defining your CUI scope with absolute precision, and be prepared for the reality that CUI must stay within a U.S.-only, fully compliant environment such as Azure Government. Trying to retrofit global IT into CMMC requirements almost always leads to unnecessary complexity. Building a segmented, purpose-built hybrid cloud solution and working with a partner that understands both the technical architecture and the compliance expectations will dramatically simplify the journey. It allows you to maintain global operations while establishing a secure, sustainable U.S. footprint for defense work.

Most importantly, don’t view CMMC as a one-time project. It’s an ongoing operational discipline. Invest early in an approach and a partner that will scale with you. The payoff is significant—greater trust from U.S. defense customers, stronger competitive positioning, and a more resilient security posture across your organization.

How would you describe your experience working with Redspin?

Working with Redspin has been an exceptional experience from start to finish. Their team brought a rare combination of technical depth, clear communication, and an understanding of what CMMC assessors actually expect. They didn’t just provide advice—they proactively worked alongside us, step by step, to design the right cloud architecture, validate configurations in our GCC High and hybrid environment, and ensure every control was fully supported with the right documentation and evidence.



“Redspin didn’t just give us advice, they were right there with us every step of the way. They really understood what assessors are looking for, and that gave us the confidence to move forward and ultimately achieve a perfect CMMC Level 2 score.”

–Patrick Lux, IS \ IT Coordinator US, NCAB Group

What stood out most was their consistency and commitment. The recurring working sessions created real momentum, and the collaborative approach made it feel like we were operating as a single team with a shared goal. Whether it was refining our policies, reviewing configurations, or preparing for the C3PAO assessment, Redspin was always organized, responsive, and grounded in practical experience.

Their guidance was instrumental in helping us achieve a perfect 110/110 and pass our CMMC Level 2 assessment. But just as importantly, they helped us build a secure and sustainable foundation for the long term. Overall, partnering with Redspin gave us confidence throughout the process and delivered exactly the support we needed to succeed.

Redspin, the federal division of Clearwater, is one of the first Authorized CMMC 3rd-Party Assessment Organizations (C3PAOs) and is the most experienced team of assessors in the ecosystem. As a trusted partner to the Defense Industrial Base, Redspin helps organizations prepare for, achieve, and sustain CMMC through training, assessments, readiness consulting, managed compliance, and secure cloud services.

From building your program to proving it—and maintaining it—Redspin protects the DIB as a service.



40 Burton Hills Blvd
Suite 410
Nashville, TN 37215

info@redspin.com
www.redspin.com
[contact us](#)