

Achieving CMMC Compliance with ERP in Your Back Pocket

By Adam Grabowski
Director of Marketing
Global Shop Solutions





Defense manufacturers today face increasing pressure to meet stringent cybersecurity requirements outlined in the Cybersecurity Maturity Model Certification (CMMC). While many understand the framework and its implications, fewer recognize how ERP systems can act as a backbone for operationalizing and documenting the controls necessary for compliance. When aerospace manufacturer Atec, Inc. pursued CMMC certification, ERP played a critical role in supporting their audit readiness.

CMMC Compliance: A Strategic Imperative for Defense Manufacturers

As CMMC requirements move toward full implementation across all Department of Defense (DoD) contracts, manufacturers must prove that they can safeguard Controlled Unclassified Information (CUI) and other sensitive data. Compliance is no longer optional – it's a prerequisite for doing business with the DoD and many prime contractors.

While many manufacturers understand the broad strokes of CMMC, the challenge lies in executing compliance and protecting sensitive information across complex systems and distributed teams. This is where ERP systems provide critical support.



ERP and CMMC: Mapping Controls to Capabilities

A modern ERP system helps bring order to the intricate requirements of CMMC. By centralizing processes and documentation, ERP enables manufacturers to demonstrate compliance in areas ranging from access control to supplier accountability.

At Atec, ERP became a bridge between policy and practice, helping them meet more than 300 individual controls required under Level 2.

“The majority of CMMC controls are focused on network security, data segregation, reporting, logging and physical security,” shares Michelle Fenley, Director of ERP & IT Systems, Atec, Inc. “Global Shop Solutions ERP’s main role in compliance revolved around the custom training program. Implementing tools, software hardware and rules throughout our network is compliance. Being able to show that users are regularly trained on all these controls is a big piece of CMMC.”

Examples of other ERP capabilities aligned with CMMC practices:

- **Audit Logging & Monitoring:** Tracks user access, changes and key system events.
- **Supplier Flowdowns:** Captures subcontractor agreements and security clauses.
- **Compliance Timekeeping:** Synchronized system clocks for an accurate timestamps in audit logs.
- **Access Control:** Enforces user roles, password requirements, and system access rules.
- **Compliance Documentation:** Produces reports and logs for auditor review.



Customer Spotlight: Atec, Inc.

When Atec, Inc. prepared for its government-certified CMMC in 2024 (after it's self-certification in 2020), its ERP system became a foundation for audit readiness. According to Fenley, the ERP software provided structured visibility into key control areas and made it easier to document compliance efforts.

"We used ERP reports and the custom training program to prove compliance," Fenley explains. "Our ERP partner created a custom certificate program within the vendor module to track agreements and contractual flowdowns to our suppliers."

Because Atec uses an on-premise ERP solution, they maintain tighter control over system security – a key consideration when protecting sensitive DoD-related data.

"As long as our network is secure, and we protect CUI as required by the 300+ controls, safety lies within the network and the tools implemented to protect the data," says Fenley.

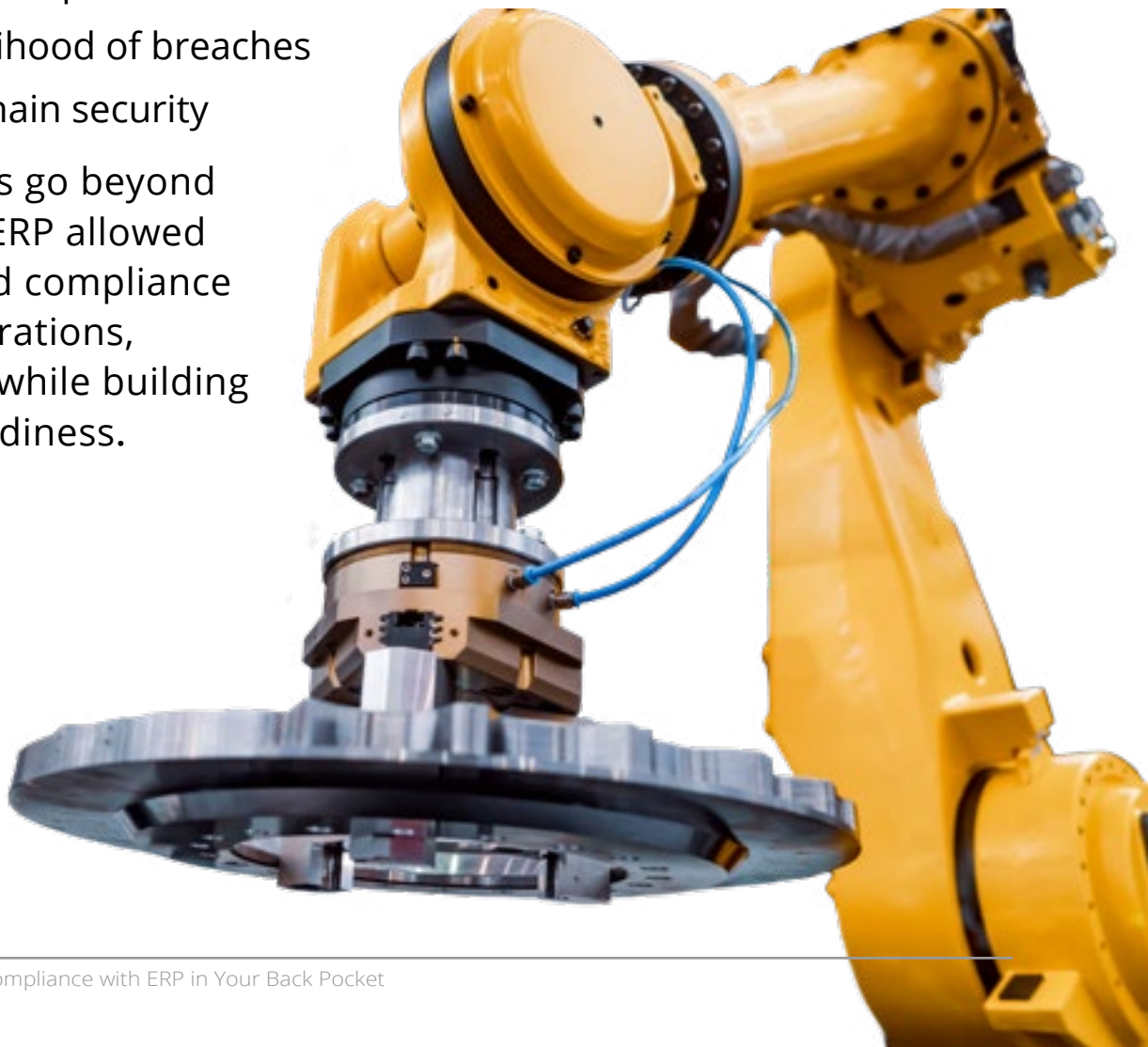


Measurable Benefits of ERP-Driven Compliance

By integrating CMMC practices within their ERP system, Atec realized operational and strategic improvements:

- Increased eligibility for DoD contracts
- Stronger cybersecurity posture
- Better risk management
- Competitive edge with prime contractors
- Improved trust and reputation
- Streamlined processes
- Less likelihood of breaches
- Supply chain security

These benefits go beyond certification. ERP allowed Atec to embed compliance into their operations, reducing risk while building long-term readiness.





“CMMC compliance is not cheap,” shares Fenley. “There are many tools, software and hardware we have implemented over the years to secure our network. And the extra security requirements may slow down a typical user. However, the cost savings and efficiency gained by NOT dealing with a cyber threat offsets from the extra cost and time it takes to have these tools in place.”

Looking Ahead: Evolving with CMMC and ERP

CMMC is being implemented in phases, with full adoption expected by 2028. For manufacturers like Atec, the ability to show cyber readiness is becoming essential even outside of DoD contracts.

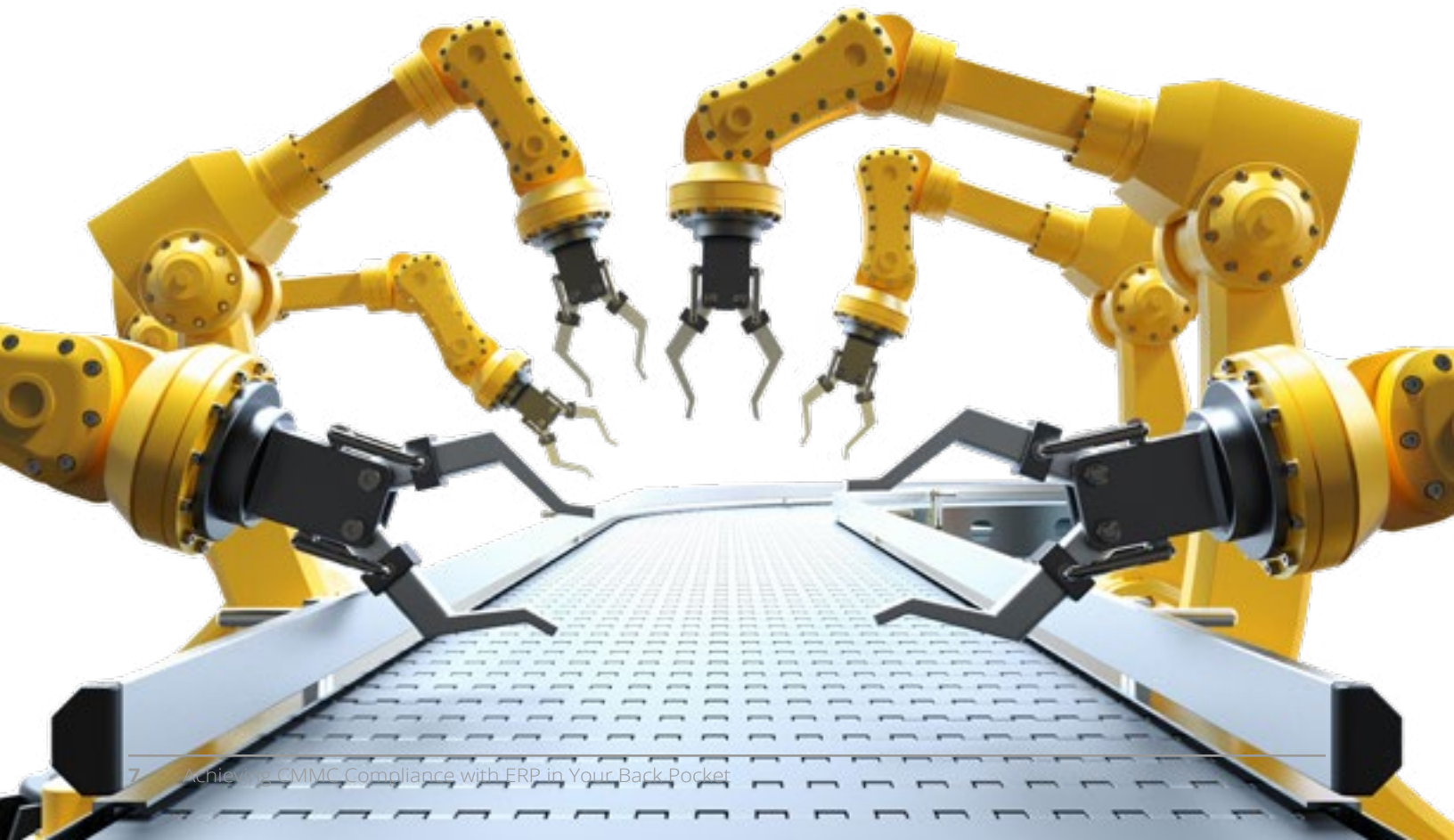
“Although they are not specified as CMMC, many large companies and primes have cybersecurity requirements that closely align with CMMC,” Fenley notes. “We are constantly answering cyber questionnaires prior to bidding with non-government agencies.”

Manufacturers that integrate compliance tools into their ERP systems will have a measurable advantage – not just in passing audits, but in winning new business.

ERP as a Force Multiplier for Compliance

CMMC isn't just about checking boxes. It's about proving your organization is serious about cybersecurity. ERP systems give manufacturers the visibility, structure, and documentation needed to make that case with confidence.

Atec's journey shows how an integrated ERP approach can turn compliance from a burden into a business advantage. For any manufacturer preparing for CMMC, the right ERP system can be the difference between delay and success.





ABOUT THE AUTHOR

Adam Grabowski is the Director of Marketing at Global Shop Solutions. He is responsible for translating the company's business objectives into successful brand, marketing and communication strategies to drive awareness, revenue and loyalty.