WHITE PAPER

Accelerating time-to-compliance: Infor CloudSuites for CMMC readiness

Navigate complex cybersecurity requirements with purpose-built technology solutions

The Cybersecurity Maturity Model Certification (CMMC) represents a critical mandate from the U.S. Department of Defense to enhance the protection of sensitive data across the complex and expanding defense contracting supply chain. Aerospace and defense manufacturers of all sizes that handle controlled unclassified information (CUI) must comply with CMMC requirements or risk losing access to lucrative U.S. government defense contracts.

While meeting the complex and rigorous CMMC standards can be extremely costly and resource-intensive for manufacturers, the purpose-built Infor CloudSuites® provide a strong foundation of capabilities to streamline and automate compliance activities. With robust role-based access control, end-to-end asset lifecycle tracking, automated workflow enforcement, and advanced analytics for predictive risk identification, Infor® CloudSuites enable manufacturers to demonstrate adherence to CMMC controls across all required domains. With decades of experience serving the aerospace and defense industries and a track record of delivering secure, certified cloud solutions for government agencies, Infor is dedicated to assisting A&D manufacturers of all sizes to navigate the path to CMMC readiness. This whitepaper explores the challenges of CMMC compliance and details how Infor CloudSuites provide an optimal platform for cost-efficient implementation of controls and processes to help manufacturers achieve certification.

CMMC 1.0

In June2020, the U.S. Department of Defense formally launched

the Cybersecurity Maturity Model Certification (CMMC) program to overhaul cybersecurity practices across the defense industrial base. The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) developed CMMC, which establishes a comprehensive framework for defense contractors and subcontractors to implement institutionalized cybersecurity controls and processes to safeguard controlled unclassified information (CUI) and Federal Contract Information (FCI) across more than 300,000 businesses that make up the defense supply chain.

This ambitious initiative aims to keep cybersecurity at the highest level across the entire defense industrial base (DIB) in response to mounting cyber threats from hostile nation-states looking to undermine America's military technological supremacy. By exploiting vulnerabilities in the supply network, adversaries have been able to steal critical data on defense technologies to shortcut years or decades of development

work.
To counter this threat, CMMC 1.0 introduced a sweeping set of controls based on NIST SP 800-171 for contractors handling CUI and sensitive defense information.

CMMC 2.0

Amajor newupgrade, CMMC 2.0, takes these requirements even further by mandating third-party audits to verify compliance, starting at CMMC Level 1. By 2025, the DOD plans to fully incorporate CMMC standards and certification requirements into all procurementrelated activities, including requests for information (RFIs), proposals (RFPs), and contract awards. Aerospace and defense manufacturers and organizations throughout the supply chain must obtain CMMC certificates at an appropriate level matching the sensitivity of the information they handle to be eligible for defense contracts.

With national security and billions of dollars in defense

business
on the line and with increasing governmental budgets on defense, the stakes are tremendously high for A&D manufacturers. The U.S. government is by far the largest global defense customer in the world.

To efficiently tackle CMMC readiness, aerospace and defense manufacturers need technology solutions purpose-built for their unique operational processes and security needs.

However, navigating this complex maze of cybersecurity requirements to achieve CMMC compliance can easily overwhelm manufacturers who rely on fragmented legacy systems, manual processes, and ad-hoc security policies. The costs to become compliant will likely exceed $100,000 for small manufacturers and are projected to top $2 million for large defense contractors. Even if such enormous surplus budgets are immediately available for investment, preparing for CMMC audits can take 12–18 months of dedicated effort, even for firms with mature cybersecurity programs.

Infor CloudSuites provide an integrated suite of applications available without costly integration or customization and designed specifically for defense contractors, including advanced capabilities to help manufacturers demonstrate adherence to CMMC requirements cost-effectively.

The challenges of achieving CMMC compliance

While the CMMC model continues to evolve, manufacturers aiming to handle CUI must already plan for compliance with over 100 cybersecurity controls at Level 2. These controls span 17 domains, including access control, asset inventory, awareness training, auditing, and system security.

For most manufacturers in the defense supply chain, significant gaps exist between their current security policies and capabilities and the upcoming requirements of CMMC Level 2 certification.

The journey to implementation

Acomplex undertaking for anymanufacturer, implementing these controls demands extensive mapping of CUI data flows to security capabilities and technical controls. It also requires significant buy-in and participation across the organization, from engineering teams securing product lifecycle management (PLM) systems to HR adopting new protocols for background checks and termination. The journey to compliance is even more daunting for small and mid-size machine shops still reliant on paper or semi-manual processes.

Successful CMMC adoption requires replacing ad hoc practices with standardized digital processes that can be consistently executed, measured, and improved. Yet generic ERP systems or custom-coded solutions offer limited abilities to automate, optimize, and simplify the assurance of CMMC controls.

The Infor solution for efficient CMMC compliance

InforCloudSuites provide purpose-builtcapabilities to help manufacturers establish the policies, procedures, and systems needed for cost-efficient CMMC adoption. With Infor CloudSuites manufacturers gain an integrated platform designed specifically for defense contractors, with functionality that maps to core CMMC domains right out of the box:

Role-based access control: Restrict data access to authorized users based on their roles and responsibilities. Easily implement the principles of least privilege and separation of duties.

Asset lifecycle tracking: Maintain end-to-end visibility into hardware and software assets which access relevant data across procurement, deployment, maintenance, and disposal.

Workflow automation: Ensure consistent, auditable execution of processes that impact CUI systems, like change management procedures.

Systems integration: Connect engineering tools like PLM and ALM to manage product data and technical documentation. Perform unified identity, access, and authentication management.

Analytics for predictive monitoring: Utilize artificial intelligence and advanced analytics to identify vulnerabilities, detect threats, and preempt compliance issues.

Four key domains for CMMC Level 2 certification

1. Access control: CMMC demands role-based access control for all users with access to CUI, following the principles of least privilege and separation of duties. Strong authentication using multi-factor authentication (MFA) is required for non-local access.

2. Asset management: Manufacturers must maintain detailed inventories of hardware and software assets that can access CUI data. This includes tracking assets across their entire lifecycle, from procurement to deployment, maintenance, and disposal.

3. Security assessments: Regular self-assessments of CMMC practices must be conducted along with vulnerability scanning, penetration testing, and (at Level 3) cyber hunt activities across CUI systems.

4. Audit logs: Detailed activity logs that record access, modifications, and deletions across CUI systems and networks must be maintained, reviewed, and protected.

Going beyond piecemeal checklists, Infor CloudSuites provide pre-built aerospace and defense domain expertise, data transparency, connectivity, and automation capabilities to optimize assurance of CMMC controls. This purpose-built solution offers faster time-to-compliance compared to generic ERP systems.

Equally important, Infor CloudSuites remain flexible and extensible. Manufacturers can adapt functionality to support their unique processes and requirements. As CMMC standards evolve, Infor's cloud delivery model ensures customers stay up-to-date via continuous updates.

Open APIs also enable customers to connect innovative applications from Infor's partners to further enhance CMMC capabilities.

Infor's commitment to security in Aerospace and Defense

With over 20 years of experience serving the aerospace and defense industries, Infor possesses unrivaled expertise in the technologies, workflows, systems, and compliance requirements unique to defense contractors.
Infor also has a strong track record of securing data for government agencies and public-sector organizations.
The U.S. Air Force, U.S. Army, and U.S. Navy use Infor's Birst analytics platform. Infor solutions carry FedRAMP, HIPAA, ISO 27001, and ITAR certifications, confirming Infor's leadership in cybersecurity.

This combination of deep industry knowledge and next-generation cloud security enables Infor to deliver purpose-built solutions aligned precisely to the complex needs of aerospace and defense. Infor maintains an unwavering commitment to continued investment in capabilities like Infor CloudSuites that are designed to accelerate CMMC adoption on the newest level and drive efficiencies around securing sensitive defense data.

Begin your journey to CMMC certification

The Cybersecurity Maturity Model Certification introduces challenging new cybersecurity requirements for aerospace and defense manufacturers of all sizes. Legacy solutions often lack the advanced, industry-specialized capabilities to demonstrate rigorous CMMC compliance across all domains.

Infor CloudSuites provide an integrated suite of applications designed from the ground up for defense contractors. With role-based access, asset lifecycle tracking, workflow automation, analytics, and more, Infor CloudSuites deliver core capabilities to optimize and speed CMMC adoption. With

decades of aerospace and defense experience, Infor is committed to leveraging cloud delivery, emerging technologies like AI, and purpose-built functionality to provide

manufacturers
with the most efficient path to CMMC readiness encompassing the upgrade challenge. Contact Infor today to learn how CloudSuites can start you on the journey to CMMC certification and safeguarding your defense contracts.

References:
1. DepartmentofDefense CMMC Model, Version 1.02
2. NIST SP 800-171 Rev 2, Protecting CUI in Nonfederal Systems and Organizations
3. Aerospace Industries Association, "CMMC 2.0: What it Means for A&D"
4. Journal of Cyber Policy, "Implementing the Cybersecurity Maturity Model Certification (CMMC)"
5. Level 2 CMMC Practices, COMPASS Cybersecurity

infor Gold Channel Partner

DECISION RESOURCES

LEARN MORE