



Navigating Security Compliance in the Construction Industry: How FedRAMP Can Help Contractors Meet 2025 CMMC Requirements

As the landscape of cybersecurity regulations continues to evolve, understanding and navigating compliance has become a daunting task for construction industry general contractors and specialty contractors. The two key regulatory frameworks in place are the Federal Risk and Authorization Management Program (FedRAMP) and the Cybersecurity Maturity Model Certification (CMMC).

Our industry increasingly relies on digital solutions, so achieving compliance with these frameworks is crucial. As the leading innovator in the construction project management space, Kahua consistently works to help make these standards more attainable for companies with far fewer technical resources.

With a better understanding of both of these frameworks, you can learn how a FedRAMP-compliant software like Kahua can facilitate compliance with the forthcoming CMMC requirements in 2025.



Understanding FedRAMP and CMMC

FedRAMP: Ensuring Secure Cloud Services for Federal Agencies



FedRAMP, established in 2011, provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services used by federal agencies.

The primary goal of FedRAMP is to ensure that cloud service providers (CSPs) meet stringent security requirements to protect federal data. FedRAMP streamlines the process for agencies to adopt cloud services, ensuring these services comply with federal security standards.

FedRAMP's requirements are based on the National Institute of Standards and Technology (NIST) Special Publication 800-53, which outlines security and privacy controls for federal information systems and organizations.

The program categorizes cloud services into three impact levels: Low, Moderate and High, each with specific security control baselines. CSPs must undergo rigorous assessment by a third-party assessment organization (3PAO) to achieve FedRAMP authorization. In January 2022, Kahua became the only full-featured project management information system (PMIS) to receive authorization.

CMMC: Enhancing Cybersecurity in the Defense Industrial Base

The CMMC, introduced by the Department of Defense (DoD), aims to enhance the cybersecurity posture of the Defense Industrial Base (DIB). This framework is designed to protect sensitive unclassified information, such as Controlled Unclassified Information (CUI), shared with defense contractors. CMMC builds upon existing cybersecurity frameworks, including NIST SP 800-171 and introduces a maturity model with three levels of cybersecurity practices.

Starting in 2025, all DoD contractors and subcontractors will be required to achieve a certain CMMC level, depending on the nature of their contracts. Unlike self-attestation, CMMC mandates third-party certification, ensuring that contractors have implemented appropriate cybersecurity measures.



Comparing FedRAMP and CMMC Requirements

Scope and Applicability	Security Control Frameworks	Assessment and Certification
FedRAMP: Primarily applies to CSPs that provide cloud services to federal agencies. It focuses on securing cloud environments and ensuring that these services meet federal security standards.	FedRAMP: Is based on NIST SP 800-53, which outlines comprehensive security and privacy controls. These controls are tailored to cloud environments and categorized into three impact levels.	FedRAMP: Requires CSPs to undergo assessment by a 3PAO and achieve authorization from the FedRAMP Program Management Office (PMO) or a federal agency. Continuous monitoring and annual reassessment are also required.
CMMC: Applies to all contractors and subcontractors within the DIB, including those in the construction industry. It covers a broader range of cybersecurity practices to protect CUI and other sensitive information.	CMMC: Builds on NIST SP 800-171 but extends beyond it to include additional practices and processes. The CMMC model comprises 17 domains with practices spread across three maturity levels, ranging from basic cyber hygiene to advanced/progressive cybersecurity practices.	CMMC: Requires contractors to undergo assessment by a CMMC Third-Party Assessment Organization (C3PAO) to achieve the required maturity level. Certification is valid for three years, with periodic reviews and updates.

How FedRAMP Compliance Supports CMMC Requirements

For construction industry contractors and subcontractors, leveraging FedRAMP-compliant software can significantly ease the transition to CMMC compliance. Here's how:

1. Alignment with Security Control Frameworks

FedRAMP's security controls, based on NIST SP 800-53, align closely with the practices outlined in CMMC. By using FedRAMP-compliant software, contractors can ensure that their cloud services already meet many of the stringent security requirements necessary for CMMC certification. As noted by Jim Reavis, CEO of the Cloud Security Alliance, "FedRAMP sets a high bar for cloud security. Achieving FedRAMP compliance inherently covers many aspects of other regulatory frameworks, including CMMC."

2. Established Processes and Documentation

FedRAMP's rigorous assessment process requires CSPs to maintain detailed documentation of their security controls and procedures. This documentation can be invaluable for contractors preparing for CMMC assessments, as you inherit some compliance features from FedRAMP.

3. Continuous Monitoring and Improvement

One of the cornerstones of FedRAMP is the requirement for continuous monitoring and regular security assessments. This proactive approach to security management aligns with CMMC's emphasis on maintaining and improving cybersecurity practices over time.

Contractors using FedRAMP-compliant software benefit from ongoing security oversight provided by their CSPs, ensuring that their systems remain secure and up to date. While creating your own program requires work, using FedRAMP-compliant software allows you to inherit some level of compliance.

4. Streamlined Vendor Management

Construction industry contractors often work with multiple vendors and subcontractors. Ensuring all parties meet CMMC requirements can be challenging. By choosing FedRAMP-compliant software, contractors can streamline vendor management processes, as these CSPs are already vetted for federal security standards.



As Katie Arrington, former Chief Information Security Officer for the Assistant Secretary of Defense for Acquisition and current VP for Government Affairs at Exiger said,

“FedRAMP provides a level of assurance that helps contractors manage their supply chain security more effectively.”

Conclusion

As the construction industry becomes increasingly digital, achieving compliance with cybersecurity regulations like FedRAMP and CMMC is essential. By leveraging FedRAMP-compliant software, construction industry contractors and subcontractors can streamline their path to CMMC compliance, ensuring that they meet the stringent security requirements necessary to protect sensitive information.

As emphasized in the industry, the synergy between FedRAMP and CMMC can provide a robust foundation for enhancing cybersecurity practices, safeguarding the construction industry’s critical assets and information.

By understanding and aligning with these regulatory frameworks, construction industry contractors can navigate the complexities of cybersecurity compliance with confidence, positioning themselves for success in the evolving digital landscape. Kahua has spent years working to achieve the highest standards in the United States, Canada, the United Kingdom and more. With our ecosystem of partners, we can be a trusted partner in your company’s journey to CMMC compliance. Find us at www.Kahua.com.

Choose Kahua

Kahua is a leading provider of capital program and construction project management software, enabling innovation that is changing the way that capital programs are planned and delivered. Global organizations use Kahua’s collaborative solution to improve efficiency, lower costs and reduce project risk throughout the entire lifecycle of their capital programs. Our purpose-built solutions for owners, program managers and contractors enable rapid implementation that minimizes time-to-value and enhances user adoption. With the industry’s only low-code application platform, customers can easily customize existing Kahua apps or even build their own new apps to run their business at peak efficiency today and rapidly adapt as business conditions dictate.

Learn more and request a demo today or email us at: connect@kahua.com



OCT 2024