

Top 10 **Technical Lessons** Learned from Kahua's Own CMMC Journey

Kahua has always had ambitious goals, but the process of obtaining FedRAMP Authorization might be one of our most challenging projects. Kahua is trusted by over 15 federal agencies, and we knew alignment with CMMC (Cybersecurity Maturity Model Certification) would be critical for our government customers to confidently deliver profitable defense projects. We wanted a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. Starting in 2025, it's required for Department of Defense contracts, meaning revenue is on the line.

The following are our top 10 tips to help you navigate your CMMC compliance journey!

- 1 Controlled Unclassified Information (CUI) is the foundation of CMMC compliance.** It touches all aspects of a platform. Many companies don't know where their sensitive information is, what kind it is, or how to keep track of it—especially when data stored in different places like the cloud or local servers. On top of that, a lot of teams don't have clear rules for protecting that information, like using encryption to lock it down. This becomes a bigger issue when sending emails, saving files, or storing data in systems that aren't fully secured.
- 2 Use multifactor authentication (MFA) to keep your information safe,** like when a code is sent to a cell phone, in addition to logging in with a password. But implementing MFA, especially on older systems or remote access tools, can be tough for companies still using outdated login methods.
- 3 Limit employees access to the tools and information they need to do their jobs.** This policy, known as the Principle of Least Privilege, protects sensitive data and reduces risk. This can be hard to manage, especially in companies where everyone has broad access by default, and lack clear rules for who should see what.
- 4 Keep data locked down during transmission—and when it's sitting in storage.** A lot of companies don't have clear rules for locking down their data, and even when they do, it's tough to make sure that protection works from start to finish. Whether in transit or at rest, data needs to be secured. That's easier said than done for many teams.
- 5 Train employees on cybersecurity best practices.** Employees themselves are often the biggest cybersecurity risk. Many aren't trained to spot fake emails, phishing, or other tricks that hackers use to get inside a company's systems. Without up-to-date awareness and training, it's easy for someone to accidentally let a threat in.
- 6 Document a plan of action in the event of being hacked or cyber threats.** Many companies don't have a plan; and even if they do, they don't practice it. Just like running safety drills on a jobsite, teams should practice what to do in a cyber emergency—before it actually happens.
- 7 Make sure vendors and subcontractors follow cybersecurity rules.** This can be tough, especially when you're working with many different companies that all handle security in their own way. It takes time and effort to ensure that everyone is doing what they should to protect your data and meet CMMC compliance.
- 8 Track what's happening across systems.** Many companies don't have clear records or regular checks, which makes it easy to miss signs of a security issue—especially when the information is spread out in different places and not monitored. Be sure to implement proper logging and monitoring solutions.
- 9 Set up computers, servers, and cloud tools properly for security.** Old software, missed updates, and mistakes in setup can leave big holes for cyberattacks. A lot of teams don't have solid backup plans in place, such as locked-down copies of their data stored safely offline, in case something does go wrong. This makes it incredibly difficult to recover.
- 10 Create clear process for handling security warnings or alerts.** When new threats pop up, it can be hard for teams to know what to do, how to share the info with the right people, or ensure that everyone is following the right steps to stay protected.