

Moving From Paralysis to Action on CMMC 2.0

Three Pathways To Get Compliant



For the 220,000 private companies that do work with the Department of Defense (DoD), time is running out. The DoD's latest version of its mandatory Cybersecurity Maturity Model Certification, CMMC 2.0, arrived in early 2023, providing a long-awaited framework to protect the public against cybersecurity threats.

While companies have known for years that certification would be mandatory, many have taken no steps toward becoming compliant—despite the fact that 80,000 contractors will require a Level 2 or Level 3 certification to continue working with the government. How serious is this requirement? Consider that Level 2 alone requires the implementation of 110 cybersecurity practices identified in the National Institute for Standards and Technology (NIST) special publication (SP) 800-17.

Under CMMC 2.0, 80,000 contractors will require a Level 2 or 3 certification to continue working with the government. How serious is this requirement? Level 2 alone requires the implementation of 110 cybersecurity practices identified in NIST special publication (SP) 800-17.

Avoidance Is Not a Solution

With rulemaking expected to be solidified within the next two years, companies that wish to continue working with the DoD have reached the last possible moment to act.

- » What is the state of your apps?
- » What is missing to make them CMMC compliant?

If you're not asking these questions, you're not moving in the right direction. And while you may be paralyzed by fear or feel overwhelmed by the mountain of work ahead of you—avoidance is not a solution. To help you move past this paralysis, we've identified three different pathways to compliance. Take a look at the three options below and decide which one best fits your scenario.





1 If time is your primary concern

Perhaps your company is quite far behind with building secure infrastructure, or you lack the experienced staff to undertake such a significant project. Regardless of your reasoning, if time is more of a concern than money, the best option is a “compliance-in-a-box” solution that offers an off-the-shelf enclave you can implement quickly and painlessly.

Compliance-in-a-box is essentially a one-size-fits-all enclave where your users can interact with DoD data. Typically, these solutions are offered by an experienced cloud provider, who will conduct intensive discovery on your current systems, listen to your needs, and then customize your solution to fit within your existing IT infrastructure. These solutions usually don't connect to central IT resources, and they do have their own incident response systems, so they won't overwhelm your IT team. Many organizations that opt for this type of infrastructure also add on managed services so they don't have to worry about ongoing compliance and system maintenance.

If time is more of a concern than money, the best option is a “compliance-in-a-box” solution that offers an off-the-shelf enclave you can implement quickly and painlessly.

Compliance-in-a-box is the straightforward option for organizations that want to take advantage of the fact that CMMC compliance is required only for the specific databases and equipment that utilize DoD data—it doesn't have to impact the rest of your IT. And when you choose to implement this solution with an experienced provider, you can rest assured they'll work quickly, so you don't have to worry about missing any critical deadlines that may affect future funding. Your provider should also include a budget for the project ahead of time, with a responsibility matrix that outlines what maintenance your IT team will manage once the environment goes live.



2 If money is your primary concern

Some organizations may have a limited budget but have already taken some initial steps toward compliance, or feel that compliance is something they can phase in over time. This is

If money matters more than time, the way forward is to work with a cloud provider to assess your current environment and build a compliant infrastructure that takes advantage of the resources you already have.

especially true if DoD work is only one aspect of the business. If money matters more than time, the way forward is to work with a cloud provider to assess your current environment and build a compliant infrastructure that takes advantage of the resources you already have. Rather than bringing in an existing solution and making minor adjustments (as you would

with compliance-in-a-box), in this case, your cloud provider creates a roadmap from scratch that charts your current IT infrastructure. You can then use that map to maximize your existing resources and reduce costs.

What does this map look like in practice? First, your cloud provider will conduct a cost assessment that compares the cost of implementing a compliance-in-a-box solution against the cost of building a custom infrastructure. Building a custom infrastructure may look less expensive initially, but you need to consider the additional cost of staff time and consulting fees. Your provider will compare these two options to optimize your timeline and ensure that you're paying only for what you truly need.

Next, your cloud team will decide whether it makes sense to build an integrated cloud environment with a CMMC-compliant section, or simply deploy a standalone CMMC-compliant solution in the cloud. In general, standalone compliant environments will cost less to build at the outset. However, integrated cloud environments are often the better investment in the long run because they allow you to optimize your current IT, manage your own CMMC-compliant enclave, and continually make use of your investment. Your cloud consultant should be able to walk you through the various options available and recommend the best custom solution for your budget.



3 If user experience is your primary concern

While time and money are the most common factors that affect decision-making around building a CMMC-compliant environment, some organizations may identify user experience as a top priority. After all, if your organization builds a CMMC-compliant system that is cumbersome, stakeholders might be tempted to find another org with more user-friendly IT. To avoid this problem, your team should enlist support from a cloud provider seasoned in user experience design to seamlessly integrate your infrastructure—whether it's a standalone solution or part of central IT. An experienced provider will take the time to get to know your users and their workflows so they can customize your solution to mirror existing business processes. Other features, like automation, can also streamline the experience for your end-users so they can spend more time doing valuable work and less time on tedious data entry.

Ultimately, user experience is a critical piece of the puzzle, no matter your budget or timeline. Choosing a cloud provider with deep knowledge of human-centered design and the ability to seamlessly integrate your secure enclave can help you avoid problems with user experience down the line. And if user experience is your top priority, you might consider partnering with a managed services provider as well to ensure that your system is always up-to-date and easy to use.

If user experience is your top priority, your team should enlist support from a cloud provider seasoned in user experience design. An experienced provider will take the time to get to know your users and their workflows so they can customize your solution to mirror existing business processes.



The Time Is Now

With CMMC 2.0 in the final stages of rulemaking, contractors have reached the moment of reckoning. In this critical moment, partnering with a provider who can lead you expertly and efficiently through the murky waters of compliance may be the most important step you make.

Compliance will require changes at every level of your system: Infrastructure, security, and application modernization. While other vendors can help identify what needs to be done, at Enquizit we conduct a gap analysis across all of those layers and fix those gaps for you. With more than two decades of experience helping both the public and private sector, we've become the go-to resource for cloud optimization and compliance for government. Make the call while there is still time to act.

Enquizit is an Amazon Web Services (AWS) Premier Consulting Partner with years of experience building compliant environments for government agencies and their vendors. To learn more about Enquizit's CMMC solutions, go to <https://enquizit.com/services/cyber-security>.

