DIY, Partner or VDI?

Choosing Your Path to CMMC Compliance

START HERE

There are four common paths for achieving CMMC Level 2. You can do the compliance work yourself. You can hire a partner to assist you while your own team does some of the work. You can hire a partner to take on the project for you. Or you can rely on VDI — virtual desktop infrastructure — to help you achieve compliance.

None of these choices is exclusive, and in practice they blend. A contractor might lead most of the work in-house and bring a partner in to help with recommendations for compliant technologies or start with a partner running everything and take on more responsibility as their understanding grows — and any of those three can run with or without a VDI enclave.

This guide walks through the advantages and disadvantages of each path, how to work out which one fits you, and how to determine if VDI is a good fit for your environment.

The paths at a glance

	DIY	Partner-directed	Partner-led	VDI enclave
INTERNAL TIME COST	Highest	High	Low	Low
WHAT IT IS	Your team implements, documents and maintains everything	A consultant tells you what to do; your team does it	An MSP or MSSP builds and runs the controls for you	CUI lives in a managed virtual desktop; the devices reaching it stay out of scope
WHO DOES THE WORK	You and your team	You, with expert guidance	The partner, with your oversight and input	The provider stands up the environment. Compliance and maintenance are yours or a partner's responsibility.
WHAT YOU NEED IN-HOUSE	Security-experienced IT, a compliance owner, a project manager, an executive sponsor	IT staff to do the work, a project manager to keep it moving	An owner for the relationship and the business decisions	An administrator, plus an owner for policies and training
WHAT DRIVES THE COST	Mostly fixed tool spend, plus internal hours. The hours are the real cost and the one people leave out	A project fee that scales with your scope. Bigger boundary, bigger engagement	Per endpoint, per month, for as long as they run your environment	High up-front cost, then a per-user subscription fee
SCOPE	Every asset that stores, processes or transmits CUI, everything that secures those assets, and anything not separated from them	Same rule. A partner helps you draw the line defensibly	Same rule, plus the partner's own systems if they handle CUI or security data	CUI is stored, processed, and transmitted only on the VDI; your endpoints are out of scope
BEST FIT FOR	Capable in-house staff, or a tight budget and time to spend	IT staff, but no compliance expertise	Little or no internal IT	Anyone with tight compliance requirements or those who prefer simplicity at a cost premium
BIGGEST RISK	Underestimating the burden or standing up and maintaining a compliant environment, documentation and evidence work	A good plan your team has no time to execute	Your partner becomes part of your assessment	Your share of the controls still has to be done

DIY

Choose it if you have IT and compliance staff who already think in security terms. In addition, you'll need the time and project management to see it through plus an executive sponsor.

Upside: lowest cash outlay, full control, and your team learns the environment deeply.

Watch out for: implementing the 110 requirements are only half the job. Writing the SSP, gathering evidence and keeping it current is where DIY projects stall.

Ask yourself: who will own this after the assessment, every year, for as long as you hold DoD contracts?

Partner-directed

Choose it if your IT team can do the work but doesn't know what an assessor expects.

Upside: expert scoping and a gap assessment up front, which prevents expensive rework and overbuying.

Watch out for: the partner advises; your team still carries the load. Budget internal hours, not just the consulting fee.

Ask the partner: how many Level 2 assessments have you helped clients through, and what happened in them?

Partner-led

Choose it if you don't have internal IT and want someone else to build and run the environment.

Upside: the least internal effort, and ongoing operations handled for you.

Watch out for: if your MSP or MSSP handles CUI or security data for you, its systems and people can come into your assessment scope. It may need its own Level 2 certification or be assessed alongside you.

Ask the partner: what is your own CMMC status, and can you give us a shared responsibility matrix showing which requirements you cover?

VDI enclave

Choose it if your organization has a tight compliance deadline, needs to manage many remote worker devices, has limited IT resources and can afford the cost premium VDI entails.

Upside: the CMMC rule recognizes that properly implemented VDI keeps the devices used to access it out of scope. Fewer in-scope assets means less to secure, document and assess.

Watch out for: VDI shrinks scope but doesn't erase your responsibilities. Policies, training and your share of the controls stay with you. Physical Protection is the one that often drops away: if all your CUI lives inside the enclave, there is nothing on your own premises to protect. If you have strong IT bandwidth, hardening your own endpoints may cost less.

Ask the provider: what documentation such as a shared responsibility matrix comes with the VDI, what do I have left to do, and have customers passed assessments on it?

Take this to your Monday meeting

Five questions. Answer each with a number or a date, not an impression.

1 **How many people handle CUI?** Not headcount — the people who open drawings, write quotes, touch test data. The smaller that group is relative to the company, the more sensible it is to build an enclave - a dedicated and isolated environment that is built to store, process and transmit CUI.

2 **How many endpoints do they use?** Laptops, desktops, phones, tablets, including home machines. Many devices for few people means hardening each one costs more than moving the people.

3 **How many locations?** One building you control is securable in place. Several sites, or everyone remote, points to an enclave.

4 **Do you have IT staff who are familiar with NIST 800-171?** Someone who configures access control, reads a log, knows what evidence an assessor wants. If no, DIY is out no matter what the budget says. If yes, but nobody knows what an assessor expects, that is partner-directed.

5 **When is the assessment, or the next award?** An actual date. Inside six months, favor whatever moves work off your team.

DIY's price tag looks like it is less expensive, which is why it wins comparisons it shouldn't. Put your internal hours in at a loaded rate before you decide.

Make sure you get answers for each of these questions.

Where PreVeil fits

PreVeil can support any of these four paths directly and works alongside the others.

PreVeil email and file sharing

Integrates with your existing environment and provides those who handle CUI an encrypted, compliant platform that keeps the part of the company not working on CUI out of scope.

PreVeil Preferred Partners

Vetted MSPs, consultants and C3PAOs for the partner-directed and partner-led paths.

PreVeil Compliance Accelerator

Supports the DIY path: assessment-ready documentation covering all 110 controls and 320 objectives, validated by an independent C3PAO. A full SSP, SOPs for all 14 control families, a pre-filled shared responsibility matrix, diagrams and checklists — needing only light customization. The Compliance Accelerator cuts documentation work by 80%.

PreVeil VDI

A managed CUI enclave running a familiar Windows desktop, so the devices used to reach it stay out of scope. It comes with a documentation package, including an SSP and a shared responsibility matrix, to shorten the path to assessment.

Sources

SOURCE	USE IT FOR
32 CFR Part 170	The CMMC Program rule, including scoping, External Service Providers and VDI
DoD CIO CMMC resources	The official Level 2 Scoping Guide and Assessment Guide
NIST SP 800-171 Rev 2	The 110 requirements every path has to meet
Cyber AB Marketplace	Directory of Registered Practitioner Organizations and C3PAOs

Prepared for CMMC Day 2026. This guide is educational and is not legal advice. Confirm your scope and approach with your assessor or RPO before you commit to a path.