G2OPS® Smarter Intelligence.®

A Practical Approach to CMMC Level 2: How We Structured Our Approach to Stay Compliant Over Time

Virginia Beach, VA, USA (30 March 2026) – When organizations approach CMMC Level 2, the focus is usually on getting through the assessment. In other words: understand the controls, implement them, document everything, and pass.

The reality, though, is that many companies aren't even at that stage yet. They are still trying to figure out where to start, how to interpret the requirements, what systems to put in place, and how to organize everything in a way that will hold up during an assessment. This proves the value of the earliest planning stages and the direction they take.

Most of the effort usually goes toward getting ready for the assessment. But if the focus is only on getting to the assessment, you can end up building something that's hard to maintain once you get there.

At G2 Ops, we made a conscious decision not to treat CMMC as a one-time event. Instead, our approach from the start focused on building the requirements into our routine operations and sustaining them.

We didn't just define policies and procedures. We focused on the recurring work required to stay compliant – reviews, checks, validations, updates, and other tasks that don't just happen once but continue indefinitely.

From there, we built our "Security Task Checklist."

At a high level, it's a set of recurring activities tied to specific CMMC controls, organized in a way that makes them assignable, repeatable, and verifiable over time.

Instead of relying on static documentation or manual tracking, we implemented this within tools we were already using to run the business. For us, that meant leveraging our existing work management and collaboration platforms rather than introducing something new.

A lot of organizations assume they need to go out and buy a purpose-built compliance tool to make this work. In our experience, that's not always necessary. Many companies are already investing in systems that can support this kind of structure, they just aren't being used that way yet.

The key is less about the tool and more about how you use it.

Within our Security Task Checklist, each recurring control-related activity became something that:

- Has a defined owner,
- Runs on a schedule,
- Produces an output, and
- Leaves a record.

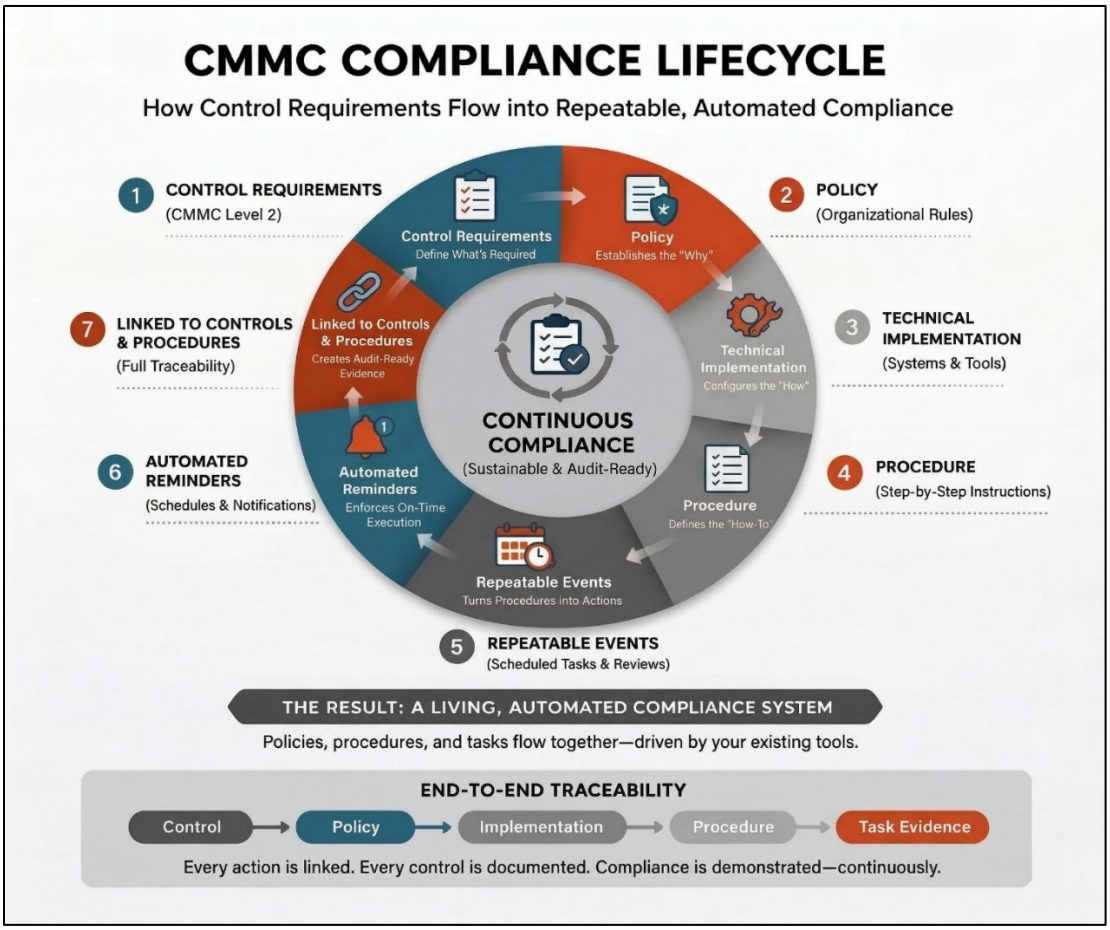
Over time, this creates a history of execution. Not something thrown together for an assessor, but something that already exists because the work is being done consistently.

It also removes a lot of guesswork. People don't have to remember when tasks are due or how they should be performed. The system reinforces the cadence through automated reminders and recurring work, which becomes especially important as the number of controls and procedures grows.

CMMC preparation results in a large set of policies, procedures, and technical implementations. Trying to manage all of that manually doesn't scale well.

We mapped out how all of this should function together cohesively, instead of letting it turn into a bunch of disconnected tasks and documents:

- Control requirements drive policy,
- Policy informs technical implementation,
- Implementation is supported by procedures,
- Procedures translate into repeatable, scheduled activities,
- Those activities are tracked and documented over time,
- Automation reinforces execution through reminders and recurring tasks, and
- All of it is traceable back to the original control.



When those pieces are connected, compliance becomes much easier to manage. You're not dealing with disconnected documents and one-off actions; you have a system where everything flows and reinforces itself.

That also makes it easier to demonstrate compliance. Instead of explaining what should happen, you can show what has been happening over time, with clear links between controls, procedures, and actual execution.

By the time we were preparing for assessment, we weren't trying to prove that we could perform the controls. We were simply demonstrating the consistency and practicality of our ongoing compliance.

I'd also like to recognize JAG Enterprises for their support and insight in helping refine this approach.

G2OPS® Smarter Intelligence.®

G2 Ops leverages over a decade of experience integrating Systems, Cybersecurity, and Software Engineering techniques to provide solutions to a growing list of Government and private customers. We combine cutting edge tools with innovative engineering practices, data analytics, and risk algorithms that enhance visibility into complex infrastructures, optimizing resiliency in system design and operations.

G2 Ops is a woman-owned small business led by an executive staff known for providing innovative solutions to solve our nation's most complex engineering challenges. G2 Ops has been named to the Inc. 5000 list of America's fastest growing companies each of the last 8 years (2018-2025) and has locations in Arlington, VA, Virginia Beach, VA, and San Diego, CA.