A REAL CMMC CERTIFICATION JOURNEY

From Policy to Proof

What leading an enterprise-wide CMMC Level 2 certification taught me about building a program from the foundation up. And what I would do now that the timeline has changed.

Tiffiney Groce
Director – Education & Compliance
Led an enterprise-wide CMMC Level 2 certification effort

WHERE WE ARE RIGHT NOW

The Timeline Changed. The Lessons Did Not.

On July 13, 2026, the Department of War suspended CMMC Phase II and opened a 60-day review. Other speakers will cover the pause. My job today is what you do with it. The house we built still stands. The inspection date is what moved.

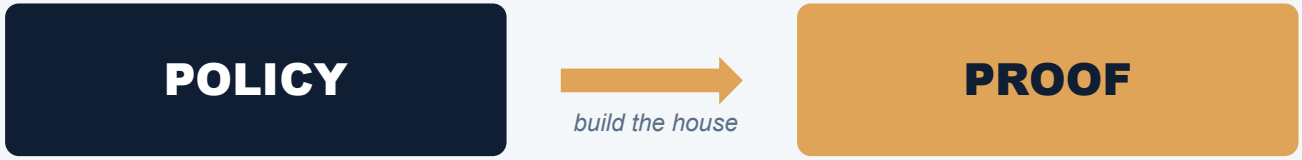
PAUSED	Phase II third-party assessments and the November 10 deadline, held in abeyance until further notice.
UNDER REVIEW	A reform task force is weighing a scalable path for small and mid-size contractors.
STILL REQUIRED	Phase I self-assessments, annual affirmations, SPRS scores, DFARS 252.204-7012, and the 110 NIST SP 800-171 Rev. 2 security requirements.
UNCHANGED	The obligation to protect controlled information. Cybersecurity risk did not pause.

"The pause changed the verification timeline. It did not remove the obligation to protect the data."

THE THROUGH-LINE

From Policy to Proof

The name of this talk is the whole journey. A policy is a decision, written down. Proof is evidence that the decision operates, every day. The distance between the two is the work.



Operational alignment What you do matches what you wrote.

Repeatable procedures Anyone can follow the same steps.

Evidence controls work Proof, generated by operating.

"Whether an outside assessor checks it or you affirm it yourself, the work still has to be proven. Documentation is the bridge between what you say you do and what you can prove."

THE ARCHITECTURE

A CMMC Program Is Built Like a House

Each layer rests on the one below it. You cannot stack proof on policies that sit on no foundation.

Before you write a policy, understand what you are protecting.

“Scope and evidence decide assessments. Not how many policies you wrote.”

If you remember one slide today, remember this one.

WHAT GOES WRONG

The Broken House

Start with policies first, and this is what eventually gets exposed, by an assessor, an internal review, a customer question, or a contract change. It is building the second floor before you pour the foundation.

Misaligned controls

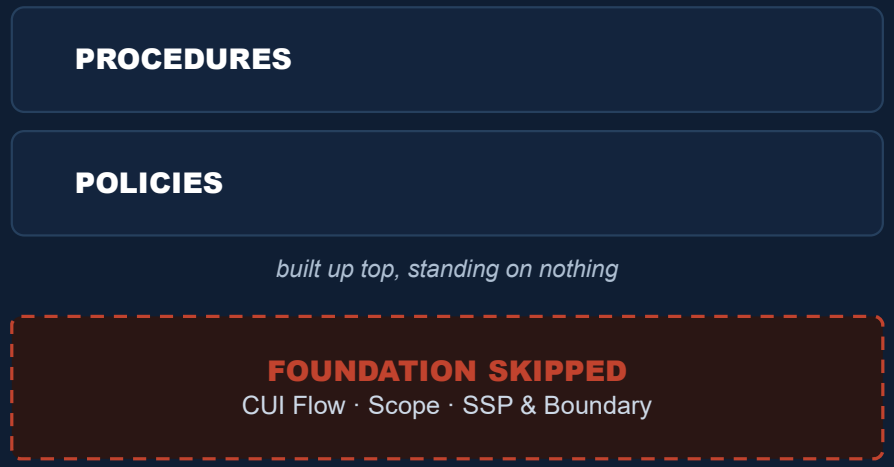
The written control does not match the environment.

Incorrect boundaries

The system boundary is wrong or undefined.

Missing evidence

Nothing proves the control actually operates.



"Starting with policies is building the second floor of a house before you have poured the foundation."

THE PERSPECTIVE SHIFT

What I Thought, and What I Learned

From leading one enterprise through Level 2, and from teaching others since, the same surprise repeats.

WHAT I THOUGHT WAS HARD

Writing the policies

Selecting the technology

Surviving the assessment

WHAT WAS ACTUALLY HARD

Scoping the environment

Identifying CUI

Managing evidence

Leading organizational change

STORM ONE

We Chose Help Before We Knew What We Needed

DIDN'T KNOW MANUFACTURING

Partners who had never worked inside an operational manufacturing environment.

OUTSIDE THEIR EXPERIENCE

They had not led an enterprise through an assessment like ours, and we could not yet tell the difference.

SOLD TEMPLATES, NOT SOLUTIONS

Generic documents off a shelf, not a program built for our environment.

“The mistake was not hiring outside help. It was outsourcing our judgment before we had built enough of our own.”

STORM TWO

We Let Price Drive the Technology Decision

THE TRAP

Choosing technology because it was the least expensive option on the table.

WHAT HAPPENED

Tools that did not support the required security outcomes or fit how our environment operated.

THE REALITY

Systems had to be replaced or upgraded later to meet the actual requirements.

“Reconsidering an investment is reasonable. Abandoning the security outcome it was meant to support is not.”

STORM THREE

We Treated Templates as a Shortcut

WHERE CUI FLOWS

No template can know how controlled information actually moves through your business.

WHAT PROCESSES IT

No template can know which of your systems store, transmit, or touch that data.

WHO ACCESSES IT

No template can know your people, roles, and access, the things you must understand first.

“A template can document a decision. It cannot make the decision for you.”

STORM FOUR

We Treated CMMC as an IT Project

SECURITY CARRIES IT ALL

When IT owns compliance alone, one team carries the entire burden.

OPERATIONS DISENGAGE

The people who actually handle CUI are never in the room.

LEADERSHIP STAYS OUT

Without ownership at the top, decisions and budget stall.

REALITY · IT TAKES THE WHOLE ORGANIZATION

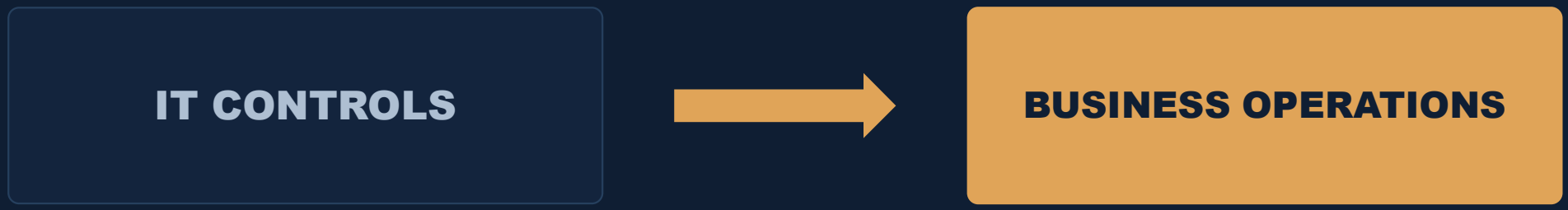
Engineering | **HR** | **Contracts** | **Supply Chain** | **Manufacturing** | **Physical Security**

“Compliance is not an IT program. It is an organizational discipline.”

THE BREAKTHROUGH

The Turning Point

The change did not come from a new tool or a better template. It came when we stopped decorating rooms and started governing the whole house, as an enterprise responsibility.



Compliance started working when the requirements were translated from IT controls into business operations.

THE OPERATING MODEL

GRC Is How You Build the House and Prove It Stands

Governance, risk, and compliance are not paperwork around the house. They are how you build it.

GOVERNANCE

The blueprint. Decides what matters, who owns it, and what the organization will accept.

RISK

The load-bearing walls. Identifies where you are exposed and what to reinforce first.

COMPLIANCE

The inspection record. Connects decisions to contracts, requirements, and evidence.

"GRC is how the organization makes, records, assigns, and defends its cybersecurity decisions."

WHO OWNS IT

Ownership Changed the Program

A house takes more than one trade. Each part of the business owns its portion.

Leadership	Decides and accepts accountability.
Compliance	Interprets, coordinates, and validates.
IT & Security	Implement the technical safeguards.
The Business	HR, contracts, engineering, manufacturing, physical security, and supply chain operate their portions.
Internal Owners	Maintain evidence and report change as it happens.

“The business decides. IT enforces. Compliance validates. Leadership stands behind the result.”

THE FIRST DECISION

Scope Was Our First Governance Decision

Scope is the footprint of the house. It is a governance decision, and it drives every one that follows.

1. What information needs protection
2. Which systems and facilities are in
3. Which people and providers touch it
4. Which controls apply
5. What the program costs
6. What evidence you must keep

“Poor scoping creates avoidable spending. Good scoping lets you protect what matters without paying to secure an environment you do not have.”

THE STANDARD TO BUILD TO

A House Built to Weather Storms

Build in this order and you get a posture, not a stack of paperwork assembled for an audit.

Documentation reflects reality

The written word and the real environment match.

Controls operate consistently

Every day, not heroics at audit time.

Evidence exists continuously

A by-product of operating, not a scramble.

“The goal is not to pass an assessment. It is a house that stands when the timeline, the assessment, or the threat changes.”

ASSESSMENT WEEK

The Open House

If you built the house right, assessment week is a walk-through. Third-party assessment is on hold indefinitely, but your contractual, SPRS, and affirmation obligations still matter. You should be able to answer these questions whether an assessor is scheduled or not.

1. Does the SSP match the environment?
2. Can employees explain their responsibilities?
3. Do procedures reflect how work is really done?
4. Can you produce evidence on demand?
5. Do controls operate consistently across the enterprise?

Whether an outside assessor arrives or you assess yourself, these are the questions to answer about your own house.

THE DECISION YOU FACE NOW

Continue, Slow Down, Change Direction, or Stop?

There is no responsible universal answer. Separate three kinds of work, then decide each on its own merits.

THE WORK	PURPOSE	EFFECT OF THE PAUSE
REQUIRED PROTECTION	Meet current contractual obligations	Generally, continues
SECURITY OPERATIONS	Reduce risk and protect the business	Continues
VERIFICATION PREP	Prepare for outside evaluation	Timing and priority may change

“If the home inspector reschedules, the roof still leaks. The date changed, not the condition of the house.”

THE PLAN

What I Would Do Now: Walk the House Again

I am not recommending a new CMMC program. I am recommending going back through the house, one layer at a time.

SCOPE	Confirm your contracts, flow-down obligations, and the CUI you actually hold.
BOUNDARY	Validate the CUI boundary and how data flows through it.
RISK	Review your posture honestly, and separate real gaps from missing documentation.
OWNERSHIP	Assign owners and realistic dates for what has to close.
OPERATIONS	Prioritize remediation by risk and contractual need, not by headlines.
EVIDENCE	Maintain evidence as processes operate; reassess verification-only spend as guidance evolves.

IF I STARTED OVER TOMORROW

What I Know Now

1. Security must be governed as a business function.
2. Scope drives cost, architecture, and accountability.
3. Tools cannot replace organizational decisions.
4. Policies must reflect actual operations.
5. Evidence should be generated by repeatable processes.
6. **Verification may change. Cybersecurity posture remains.**

THE QUESTION TO TAKE BACK

When the Assessor Arrives, You Open the Door

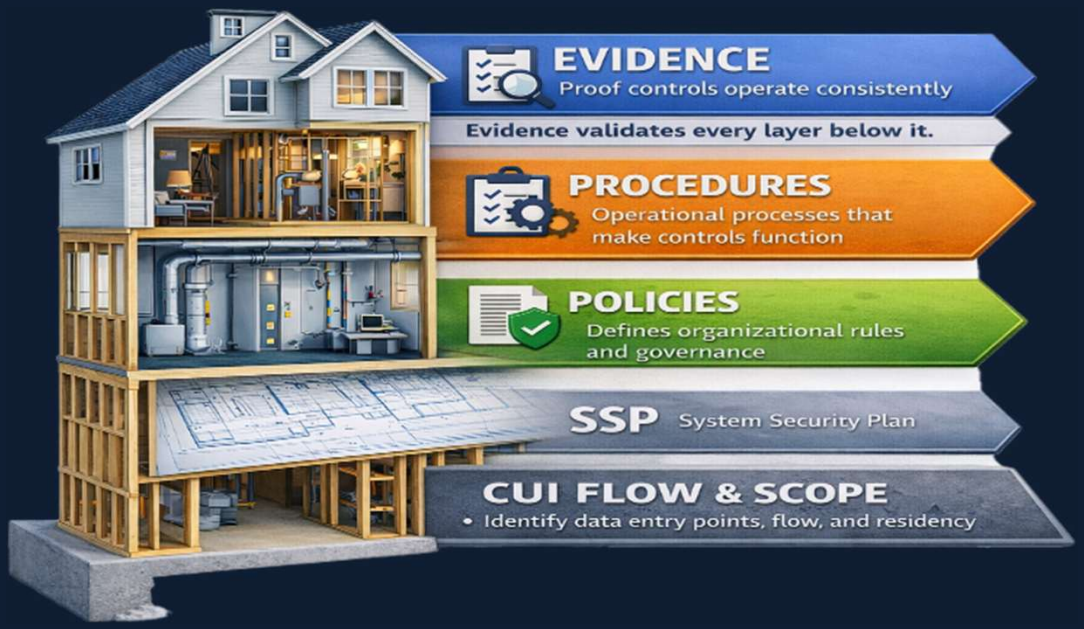
Do not build a cybersecurity program only because an assessor may arrive. Build one because your organization needs to understand what it protects, who owns the risk, and whether its claims are true.

> *"If no outside assessor came for the next two years, would your organization keep doing the work?"*

That is the question I want you to take back.

Thank You

Let's talk. **Q & A**

Tiffiney Groce

Director – Education and Compliance