CMMC STRATEGY CHECKLIST:

COMMON MISTAKES AND HOW TO AVOID THEM

Use this checklist as a quick self-assessment when building or reviewing your CMMC program.

1. Waiting for Perfect Rule Clarity

The mistake: Many organizations delay action while waiting for final rule details or additional guidance.
Why it causes problems: The CMMC landscape will continue to evolve. Waiting typically leads to rushed implementation when a contract requires certification. In addition, prime contractors are already requiring CMMC "flow down," and the rule is officially in effect.
How to avoid it:

- Start with current guidance and best practices
- Engage experienced advisors early
- Build a program that can adapt as requirements evolve
- Focus on readiness, not perfect timing

2. Treating CMMC as a Compliance Exercise Only

The mistake: Organizations approach CMMC as a checklist instead of a strategic business decision.
Why it causes problems:
CMMC directly affects:

- Contract eligibility
- Cost of compliance
- IT architecture
- Growth strategy

How to avoid it:
Before implementing controls, clarify:

- Which contracts you plan to pursue
- Whether your environment includes FCI or CUI
- Whether actual CMMC cost of compliance will support your planned growth

3. Under-Scoping the Environment

The mistake: Trying to limit scope to reduce cost by assuming CUI is not present.
Why it causes problems:
CUI often spreads through normal business processes:

- Emails and attachments
- Engineering artifacts
- Shared drives
- Derivative documentation

If discovered later, organizations may face:

- Re-scoping
- Additional assessments
- Increased cost

How to avoid it:

- Map where CUI originates
- Identify where it is stored, processed, and transmitted
- Trace how it propagates through workflows

4. Over-Scoping the Environment

The mistake: Including the entire enterprise in scope "just to be safe."

Why it causes problems:

Over-scoping dramatically increases:

- Implementation cost
- Operational complexity
- Assessment scope
- Compliance timelines

How to avoid it:

Choose the right architecture strategy:

- Enterprise Scope - Best for complex organizations with broad CUI flows
- Enclave Scope - Best when CUI can be clearly isolated

Make the decision based on actual data flows, not assumptions.

5. Buying Tools Before Defining Ownership

The mistake: Purchasing security tools before assigning responsibility for controls.

Why it causes problems: Technology alone does not satisfy CMMC requirements.

Controls must be:

- Implemented
- Maintained
- Monitored
- Documented

Tools may also not be fit for their intended purpose, even if CMMC compliance is achieved.

How to avoid it:

Before selecting tools:

- Assign control owners
- Define process workflows
- Identify required evidence artifacts
- Engage stakeholders throughout the organization

Technology should support the process — not replace it.

6. Treating the SSP as Paperwork

The mistake: Creating a System Security Plan (SSP) simply to satisfy documentation requirements.

Why it causes problems: Assessors evaluate what your SSP says you do — and then verify that it actually happens. If your SSP doesn't match your environment, the assessment will fail.

How to avoid it:

Treat the SSP as your operational blueprint:

- Document how controls actually work
- Align processes with what is written
- Maintain the SSP as a living document

7. Building the Environment to Fit Existing Systems

The mistake: Trying to force CMMC requirements to fit current infrastructure.

Why it causes problems: Organizations often end up rewriting documentation to justify existing systems instead of implementing compliant controls.

How to avoid it:

Design with the assessment in mind:

- Define required artifacts first
- Validate control capabilities before implementation
- Ensure solutions meet requirements (e.g., encryption standards)

8. Not Defining Data Flow and Scope Early

The mistake: Starting implementation before understanding where sensitive data flows.

Why it causes problems:

Assessors first evaluate:

- Data flow diagrams
- Asset inventory
- Boundary definition

Without these, scope becomes unclear and assessments become difficult.

How to avoid it:

Early in the program:

- Create a CUI data flow diagram
- Develop a complete asset inventory
- Clearly define system boundaries

9. Treating Readiness as a Date Instead of a Capability

The mistake: Setting an assessment date before the program is mature.

Why it causes problems: Organizations repeatedly delay assessments because controls and evidence are not ready.

How to avoid it:

Focus on continuous readiness:

- Plan backward from contract timelines
- Include remediation time in roadmaps
- Validate controls regularly

10. Failing to Build Evidence from Day One

The mistake: Trying to gather documentation right before the assessment.

Why it causes problems: CMMC assessments require proof that controls operate consistently over time. Intent is not evaluated — evidence is.

How to avoid it:

Design processes that automatically generate proof:

- Log monitoring
- Ticketing systems
- Change management records
- Centralized evidence storage

Practical First Steps:

Organizations preparing for CMMC should prioritize three early actions:

1. Define scope and data flows

- Identify CUI and FCI
- Map how data moves through the environment

2. Establish governance

- Assign control owners
- Define reporting cadence

3. Build audit-ready processes

- Align documentation with operations
- Implement evidence collection workflows

Ready to schedule a CMMC assessment?

Reach out to Robyn Barton, Shareholder, LBMC Cybersecurity, robyn.barton@lbmc.com.