

Cyber Resilience

# Converting Compliance Into Advantage

October 2026

forvis mazars

# Today’s Presenters



**Tom Tollerton**
Principal, IT Risk & Compliance
704.367.7061
tom.tollerton@us.forvismazars.com



**Alex Imani**
Senior Manager, IT Risk & Compliance
704.367.7093
alex.imani@us.forvismazars.com



© 2026 Forvis Mazars, LLP. All rights reserved.

# Agenda

1. Board Expectations & Outcomes-Based Security
2. Security Controls and Business Outcomes
3. NIST CSF vs. CMMC
4. CMMC Fundamentals & Program Timeline
5. CMMC Readiness, Assessment, & Evidence
6. The FAR CUI Rule





© 2026 Forvis Mazars, LLP. All rights reserved.

# Board Expectations & Outcomes-Based Security
## Why This Matters Now

- Cybersecurity is shifting to become a capability that can help organizations protect contracts, operations, and mission outcomes
- At the board level, leaders want assurance that programs can protect revenue, safety, and contractual eligibility
- The risk landscape is expanding with AI-enabled threats, supply chain exposure, and shifting requirements widening the gap between compliance and true preparedness




© 2026 Forvis Mazars, LLP. All rights reserved.

# Board Expectations & Outcomes-Based Security

## What Leaders Expect

### Risk Reduced, Not Boxes Checked

Evidence that investments can measurably reduce business risk and improve resilience.

### Critical Systems & Operations Protected

Assurance around revenue, safety, intellectual property, and contract eligibility.

### Decision-Ready Insight

Metrics that translate technical status into choices leaders can make decisively.

### Confidence Amid Change

A repeatable approach that holds up as requirements and threats evolve.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# Security Controls Mapped to Business Outcomes
## A Model

| Security Control | | Business Outcome |
|---|---|---|
| **Access Control & MFA** | » | Helps protect Controlled Unclassified Information (CUI) and contract eligibility |
| **Continuous Monitoring** | » | Helps detect issues before they disrupt operations |
| **Incident Response Readiness** | » | Limits downtime and cost when events occur |
| **Supply Chain Flows** | » | Reduces third-party risk across the business |


© 2026 Forvis Mazars, LLP. All rights reserved.

# NIST CSF vs. CMMC
## Benchmarking vs. Conformity

| NIST CSF 2.0 — VOLUNTARY | | CMMC — MANDATORY |
|---|---|---|
| Voluntary benchmarking across six core security functions | PURPOSE | Mandatory conformity assessment against the NIST SP 800-171 requirements |
| Measures the maturity of the enterprise security program as a whole | SCOPE | Verifies specific requirements inside a defined CUI assessment boundary |
| Self-directed; the organization sets its own target profile | ASSURANCE | Assessed by a C3PAO or self-assessed, then affirmed annually in SPRS |
| Answers “how strong is our program?” | BOTTOM LINE | Answers “can we prove eligibility for this contract?” |


© 2026 Forvis Mazars, LLP. All rights reserved.

# CMMC Fundamentals
# What It Is & Who It Applies To

## A Certification Program

**32 CFR Part 170**

CMMC verifies that defense contractors protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) on their own systems.

## Three Levels

**Scaled to Sensitivity**

Level 1 covers basic FCI safeguarding, Level 2 the 110 NIST SP 800-171 requirements for CUI, and Level 3 the most sensitive programs.

## A Condition of Contract

**Primes and Subcontractors**

Required status flows down the supply chain and, when in force, becomes a condition of award under DFARS 252.204-7021.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# Inside the CMMC Program

CMMC is the DoW's framework for verifying that its supply chain protects sensitive information.

## Why the Program Exists

Repeated supply chain compromises pushed DoW to verify contractor security instead of accepting self-attestation.

## Who It Reaches

A Defense Industrial Base estimated at more than 200,000 organizations, across every size and industry.

## What It Protects

Controlled Unclassified Information: broad categories sensitive to DoW but below classified, and often ambiguously marked.

## Who Runs It

The DoW owns the program, the Cyber AB accredits assessors, and authorized C3PAOs perform the assessments.

forvis mazars

# CMMC Fundamentals
# The Underlying Requirements

CMMC does not create new controls. A Level 2 assessment measures NIST SP 800-171 as written.

**1**

## Structure

110 security requirements organized into 14 control families.

**2**

## Objectives

NIST SP 800-171A expands those into 320 discrete assessment objectives.

**3**

## Evidence

Each objective is proven by policy, configuration, or operational records.

## What the Families Cover

- Access control, identification, and authentication for users and devices
- Audit and accountability, configuration management, and system integrity
- Incident response, media protection, and physical protection of CUI
- Awareness and training, personnel, risk, and security assessment



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# CMMC Fundamentals
## How the Program Has Unfolded

The underlying requirements have been steady; the enforcement schedule is what keeps moving.

**Dec 2024**

The CMMC Program Rule (32 CFR Part 170) took effect, standing up the assessment ecosystem and authorizing C3PAOs.

**Nov 2025**

The acquisition rule (DFARS 252.204-7021) took effect, starting a phased rollout with Level 1 and Level 2 self-assessments.

**July 2026**

The Department suspended Phase 2, which would have required C3PAO certification, and stood up a CMMC reform task force.

**Today**

Phase 1 self-assessment obligations and annual SPRS affirmations remain in force while the program is under review.





© 2026 Forvis Mazars, LLP. All rights reserved.

# CMMC Readiness, Scoping, & Evidence
# **Scope With Confidence**

Scope drives cost, complexity, and credibility. Start by identifying where CUI exists.

**1**

## Identify

Locate each place CUI is processed, stored, or transmitted.

**2**

## Validate

Confirm defensible system and organizational boundaries.

**3**

## Document

Capture an accurate asset inventory and data flow diagram.

## Right-Size the Boundary

- Too broad pulls non-CUI assets into scope and inflates cost and effort
- Too narrow undermines credibility and invites assessor questions
- An enclave can segment CUI assets from out-of-scope systems
- Scope changes ripple into fees and previously reviewed controls



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# CMMC Readiness, Scoping, & Evidence
# **Build the SSP, Then the Evidence**

## What Strong Evidence Looks Like

1. **Owned**
   Each artifact has a clear, accountable owner.
2. **Current**
   Refreshed on a defined cadence, ideally under six months old.
3. **Repeatable**
   Generated by routine operations, not reconstructed after the fact.
4. **Tied to an Outcome**
   Defined by the question it answers, not simply the document title.

### Document First, Then Organize

- Build the SSP first: control status, implementation, ownership, and inheritance
- Version-control the SSP and re-approve it at least annually
- Give special attention to “defined” and “specified” objectives


© 2026 Forvis Mazars, LLP. All rights reserved.

# CMMC Readiness, Scoping, & Evidence
## Closing the Loop

### Self-Assessment

**Level 1 & Some Level 2**

Score the requirements against the assessment objectives, post the result to SPRS, and stand behind it.

### Independent Assessment

**C3PAO Certification**

An authorized third party validates the same evidence and issues a certification the Department recognizes.

### Either Path

**Affirm & Maintain**

A senior official affirms annually, POA&M items close on schedule, and evidence keeps flowing from daily operations.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# CMMC Readiness, Scoping, & Evidence
## How to Run the Self-Assessment

Assess against the NIST SP 800-171A objectives, not the requirement summaries; that is where missteps can happen.

### Confirm Scope

Fix the assessment boundary first: the systems, people, and providers that handle CUI, plus any inherited controls.

### Test Controls

Work all 110 requirements objective by objective, using the SSP and evidence. Each one is MET or NOT MET; no partial credit.

### Score & Plan

Apply the DoW 110-point methodology, then build a POA&M with named owners and closure dates for every NOT MET objective.

### Post & Affirm

Post the score, scope, and assessment date to SPRS; the senior affirming official then affirms accuracy annually.





© 2026 Forvis Mazars, LLP. All rights reserved.

# Maintaining Readiness Between Assessments

Readiness decays if it’s not maintained. Watch the areas that quietly erode a program.

### Monitor Changes to the Environment

Major changes may require re-assessment; watch CUI ingestion, marking, and placement.

### Flow Requirements Down the Supply Chain

Integrate obligations into vendor management so subcontractors stay aligned.

### Affirm Accurately Each Year

Leadership affirmation should reflect reality; keep evidence current to support it.

### Maintain Business-as-Usual Operations

Ongoing training and vulnerability management help keep controls from drifting.

forvis mazars

# Why Pursue CMMC Level 2 Voluntarily

With Phase 2 paused, certification is optional today, which is exactly what makes it a differentiator.

### Independent Validation

A third-party assessment provides objective evidence that your security baseline is real, not self-declared.

### Potential Liability Protection

Independent evidence of compliance helps mitigate False Claims Act exposure tied to annual SPRS affirmations.

### Contract Positioning

Certification signals readiness to primes and program offices before requirements return to solicitations.

### Schedule Certainty

Assessor capacity is finite, so certifying early avoids the queue when phased requirements resume.

forvis mazars

# The FAR CUI Rule
# **What It Would Require**

Still proposed, the rule would standardize CUI handling across every federal agency, not just DoW.

**1**

## Identify

A standard form would name the CUI categories involved and the handling required on each contract.

**2**

## Safeguard

Protection requirements would draw on NIST SP 800-171, so existing CMMC work carries over directly.

**3**

## Report

Contractors would notify the agency on a set clock when CUI is compromised.

## What Else to Watch

- Reaches civilian agency contracts that never fell under DFARS 252.204-7012
- Requires CUI training for personnel before contract performance begins
- Flows the same obligations down to subcontractors at every tier
- Comment period closed in March 2025; the final rule remains pending



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# CMMC at Forvis Mazars

As one of the earliest Authorized and Accredited C3PAOs, we have completed over 100 CMMC L2 assessments and are proud to bring the following value-added contributions to the program.

Forvis Mazars has performed over 100 CMMC L2 assessments for contractors of all sizes and industries. With an experienced CMMC Consulting team, our firm can provide support with the following:

- CMMC L2 Certification Assessment
- CMMC L2 Self-Assessment Support
- CMMC L1 Readiness Support
- CMMC Compliance Program Development
- CMMC Gap and Mock Assessments
- CMMC Revision 3 Gap Assessment
- System Security Plan Development
- POA&M Development and Remediation Advisory
- Technical Assessment and Penetration Testing






© 2026 Forvis Mazars, LLP. All rights reserved.

# Cybersecurity & Compliance Services
# **Forvis Mazars Stands Ready to Assist**

## Gap & Mock Assessments

Find and prioritize gaps before the assessment that counts.

## Security Plan Development

Build an accurate SSP that reflects the environment you run.

## POA&M & Remediation

Turn findings into a focused, defensible closure plan.

## CMMC Program Development

Maintain a cybersecurity posture that aligns with current requirements.

## Penetration Testing

Validate that controls perform under real-world conditions.

## Readiness & JSVA Support

Build a Joint Surveillance Voluntary Assessment (JSVA) program and prepare for what's next with an experienced team.



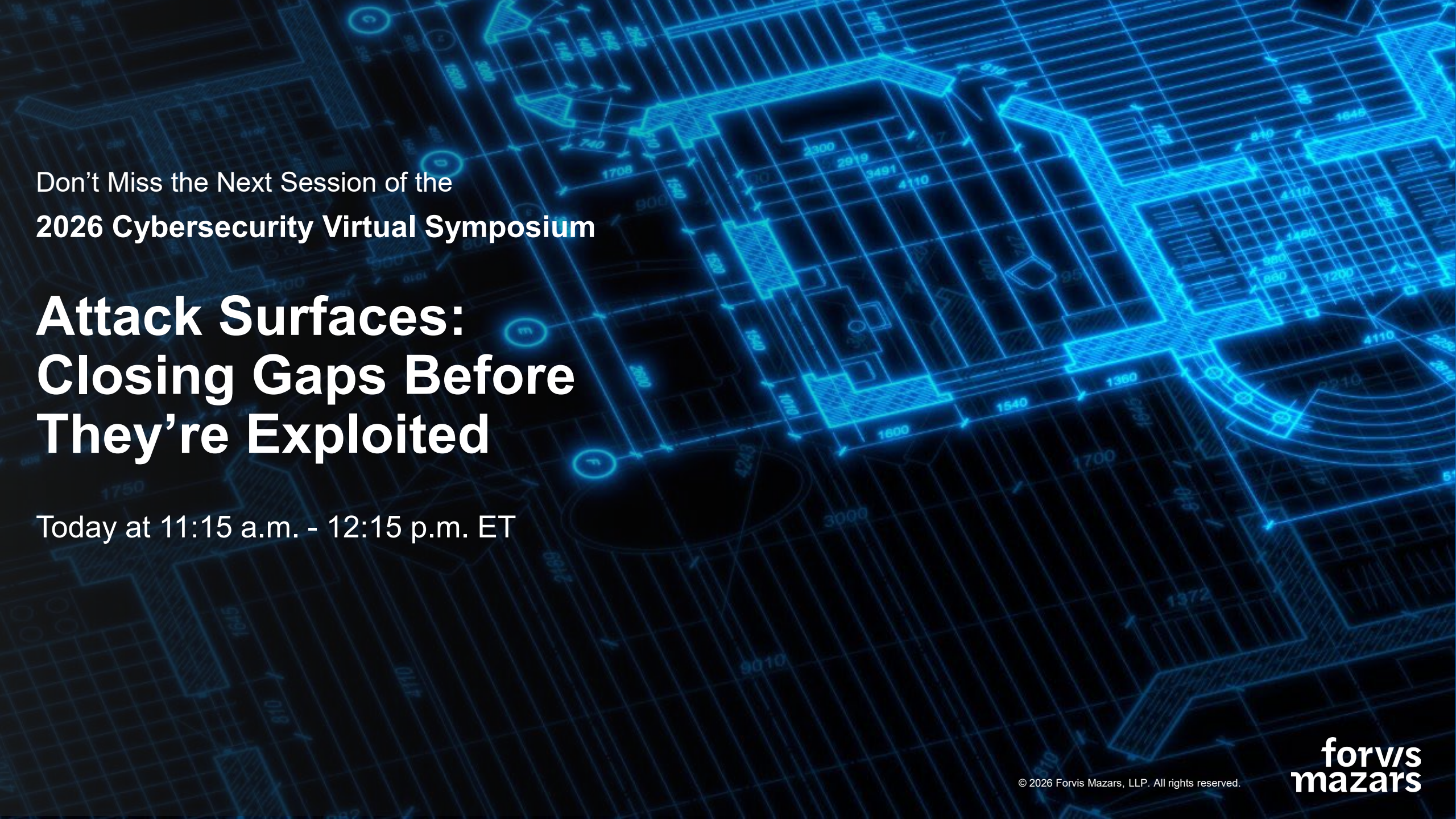


IT Risk & Compliance

# Questions?



© 2026 Forvis Mazars, LLP. All rights reserved.



Don’t Miss the Next Session of the

**2026 Cybersecurity Virtual Symposium**

# Attack Surfaces: Closing Gaps Before They’re Exploited

Today at 11:15 a.m. - 12:15 p.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

# Contact


## Forvis Mazars

**Tom Tollerton**
Principal, IT Risk & Compliance
P: 704.367.7061
tom.tollerton@us.forvismazars.com

**Alex Imani**
Senior Manager, IT Risk & Compliance
P: 704.367.7093
alex.imani@us.forvismazars.com



The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.