Pittsburgh Chapter ISSA
Information Systems Security Association

A Clear Path to NIST & CMMC Compliance

NIST 800-171 & CMMC 2.0 Compliance Update

Jack Nichelson
Chief Information Security Officer
Inversion6

Jack Nichelson

i6 CISO
ELIMINATE REACTIVE

- Recognized as one of the “People Who Made a Difference in Security” by the SANS Institute and Received the CSO50 award for connecting security initiatives to business value.
- Adviser for Baldwin Wallace’s, State winner Collegiate Cyber Defense Competition (CCDC) team.
- Certs: Executive MBA, CISSP, CCNA, GIAC GCIH, GIAC GSLC, CCNP, CCDA, & VCP
- Prior experience running Infrastructure & Security at multiple Fortune 500’s
- 20+ years in IT & IT Security
- Board member for FBI InfraGard
- Executive MBA from Baldwin-Wallace University

TruWest Family of Companies

TRUWEST HOLDINGS

TRG	Inversion6	RIVER CAPITAL FINANCE	RIVER SaaS CAPITAL	SIBLING REVELRY BREWING
Point of Sale (POS) Lifecycle Management	Custom cybersecurity solutions	IT and AIDC equipment financing	Venture debt for SaaS businesses	Craft kitchen and taproom

REPRESENTATIVE CUSTOMERS

AMERICAN GREETINGS · BakerHostetler · borchers · CBIZ · Cleveland State University 1964 · EQUITY TRUST COMPANY · HAHN LOESER · Ohio CAT

oswald · Pat Catan's CRAFT CENTERS · REAL ALLOY · SHILOH · Summa Health · Sunshine CREATING COMMUNITY · TA · THOMPSON HINE · windstream

CMMC Fundamentals

Recap from CMMC 2021-22

Introduction to CMMC

- **The Cybersecurity Maturity Model Certification or CMMC** is a unified standard designed to improve cybersecurity across the thousands of companies in the Defense Industrial Base (DIB)
- **The new model will verify that DoD contractors have sufficient controls** to safeguard sensitive data, including Confidential Unclassified Information (CUI) and Federal Contract Information (FCI).

CMMC is an evolution of the DFARS 252.204-7012, 7019, 7020 and 7021 regulations requiring compliance with NIST 800-171

Key CMMC Acronyms

Defense Federal Acquisition Regulation Supplement (DFARS):

DFARS Regulations 252.204-7012, 7019, 7020 and 7021 call for protection of CUI based on NIST 800-171

System Security Plan (SSP):

The document that identifies the functions and features of an organization's compliant system, including all its hardware and the software installed on the system

Cybersecurity Maturity Model Certification 2.0 (CMMC):

CMMC is the US Government's solution to fix low rates of compliance associated with NIST SP 800-171

Federal Contract Information (FCI):

FCI is information provided by or generated for the Government under contract not intended for public release

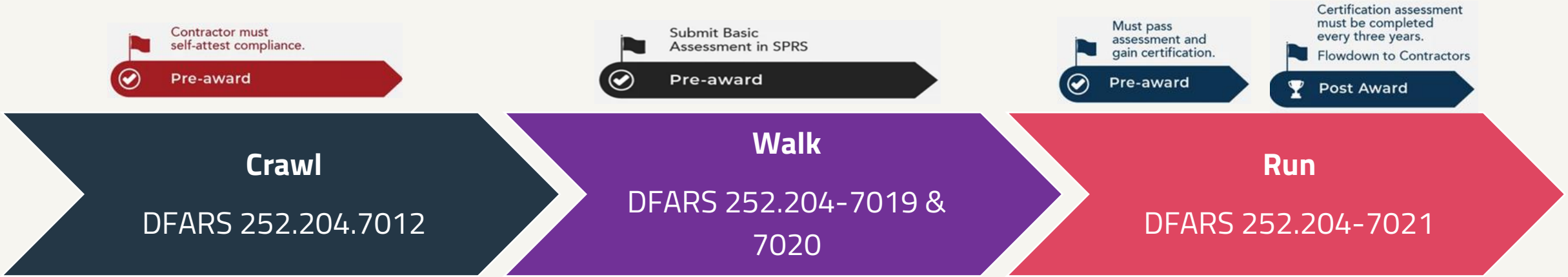
Controlled Unclassified Information (CUI):

CUI is an umbrella term that encompasses all Covered Defense Information (CDI) and Controlled Technical Information (CTI)

Certified Third-Party Assessment Organization (C3PAO):

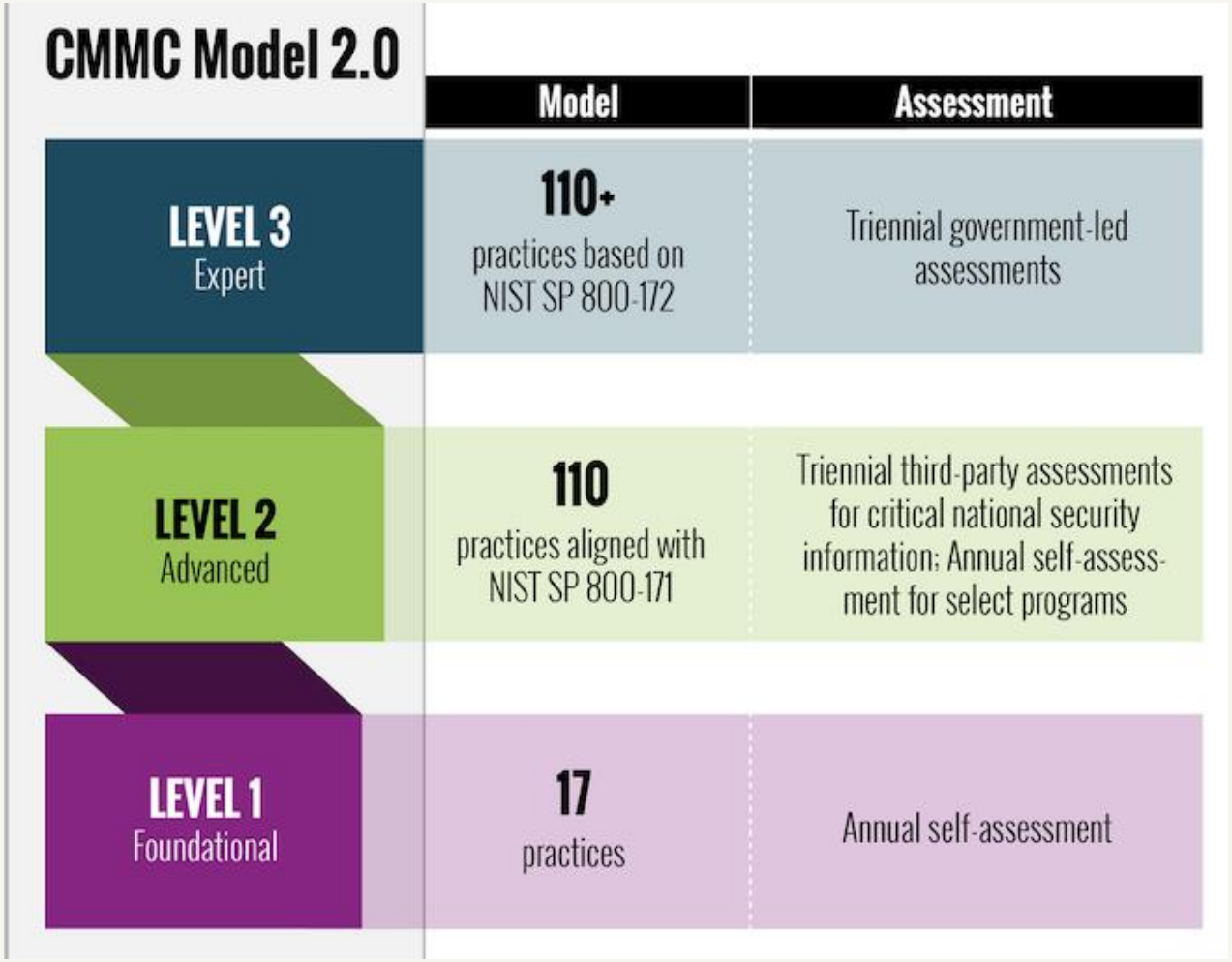
C3PAO is an organization authorized by the CMMC-AB to conduct, and deliver CMMC assessments

CMMC is built on DFARS



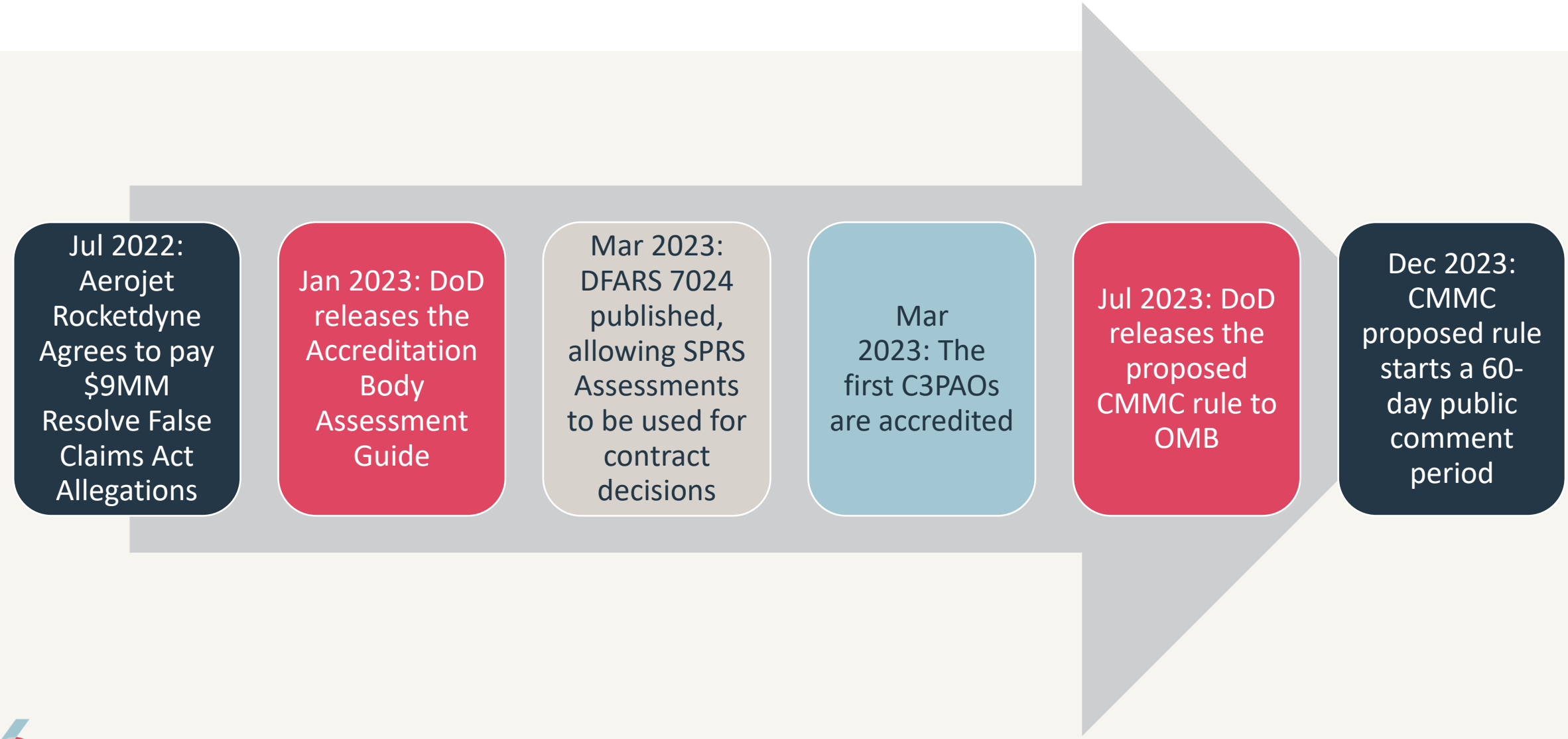
- **Crawl**: **DFARS 252.204-7012**, also known as Safeguarding Covered Defense Information and Cyber Incident Reporting. Requires defense contractors to provide adequate security by implementing the 110 security controls in NIST 800-171 and self-attest this has been done. **This clause went into effect end of 2017**.
- **Walk :** **DFARS 252.204-7019 & 7020**, are clauses that outline the requirements for contractors to comply with NIST 800-171. It requires contractors to maintain a record of their NIST 800-171 compliance with a System Security Plan (SSP) and registering a CAGE code in the Supplier Performance Risk System (SPRS). This is not "graded", but the DFARS rule does articulate the risk of False Claims Act (FCA) litigation if not done in earnest. **These clauses went into effect on November 30, 2020**.
- **Run:** **DFARS 252.204-7021**, also known as "Cybersecurity Maturity Model Certification Requirements", is a clause that outlines the requirements for contractors to comply with the Cybersecurity Maturity Model Certification (CMMC). This is when CMMC controls, processes, & practices become required elements for doing business with the Department. **This clause will go into effect October 2025**.

What You Need to Know About CMMC 2.0

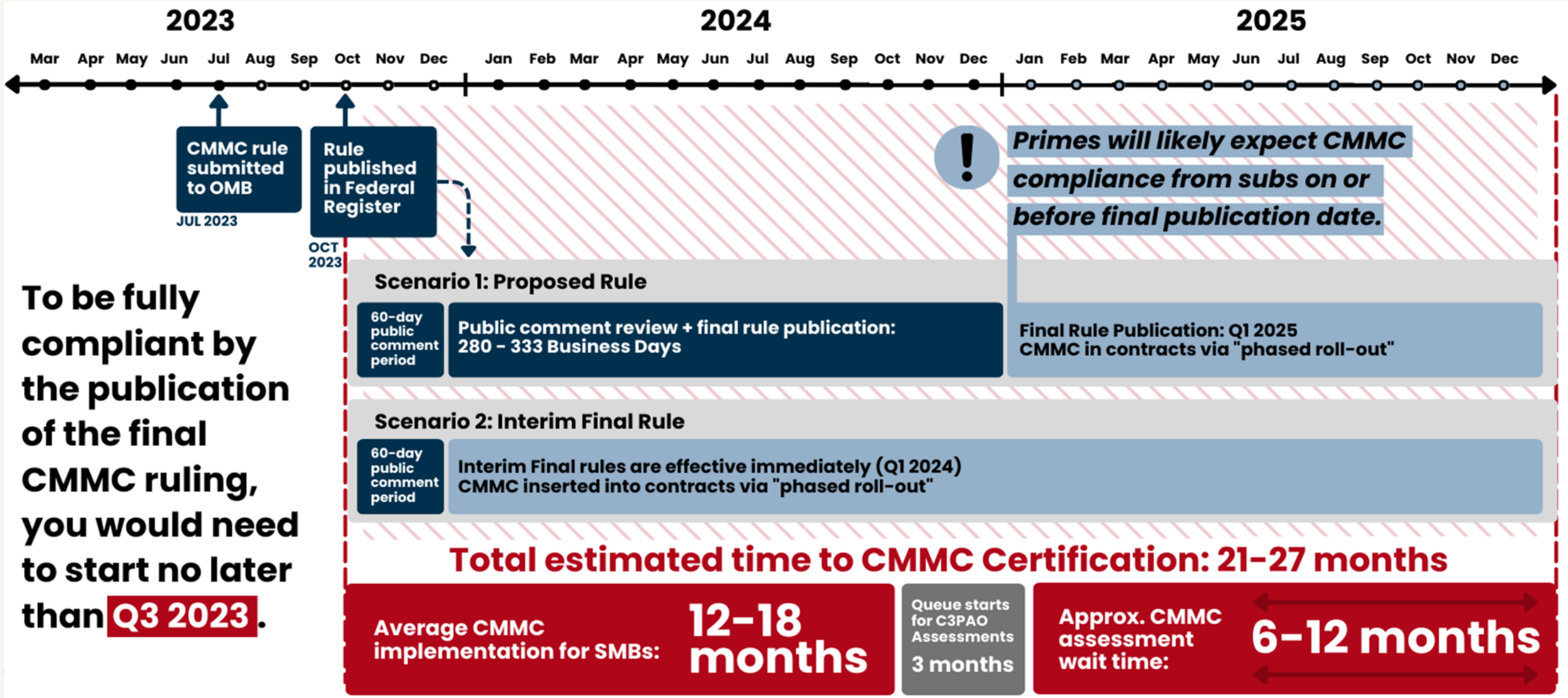


- All members of the DIB are subject to the Defense Federal Acquisition Regulation Supplement (DFARS) rules, which require meeting NIST 800-171
- NIST SP 800-171 is completely aligned with Level 2 of CMMC 2.0
- All DoD contractors will have to ensure all subs are CMMC compliant (a.k.a. “Flow Down”)
- CMMC compliance will be phased into contracts in 2025

Recent Key Events in CMMC's Timeline



Timeline for CMMC Adoption



To be fully compliant by the publication of the final CMMC ruling, you would need to start no later than Q3 2023.

Call to Action

Enough! It’s time to get sh⓲t done!

A Simple Framework

Plan: Establish objectives and goals

- This stage focuses on identifying the problem or opportunity for improvement, setting specific targets, and planning how to achieve them.

Do: Implement the planned actions

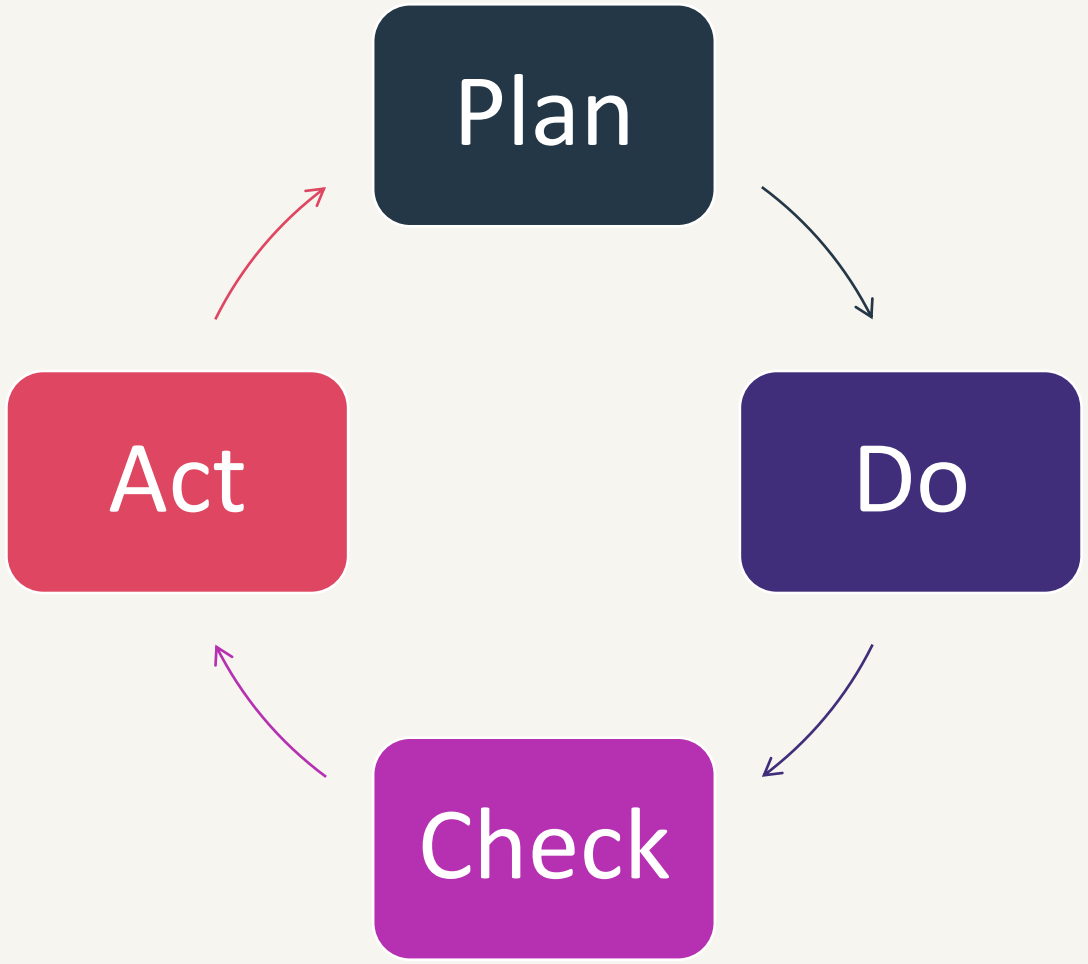
- This stage involves carrying out the planned activities, starting with a pilot project or small-scale test.
- It's a hands-on phase where you put your plan into action.

Check: Assess and monitor the results

- Compare the actual outcomes to the expected outcomes and gather data to evaluate the effectiveness of the changes.

Act: Make decisions and take actions

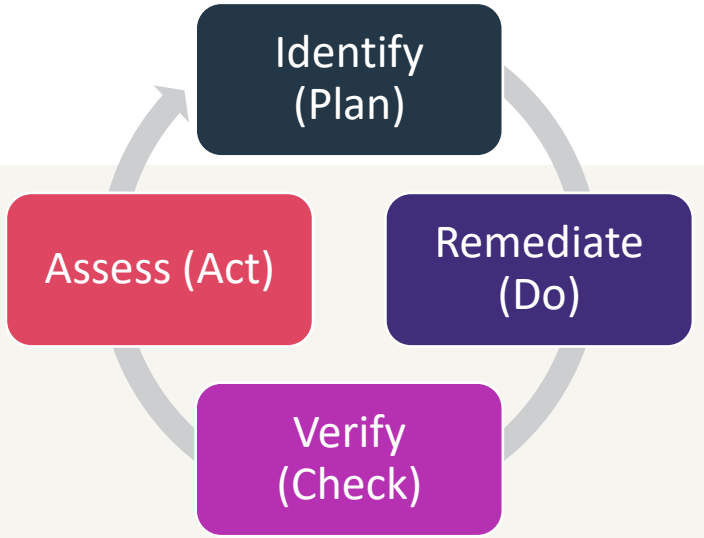
- If the results align with your objectives and goals, you standardize the improvements, update processes, and continue monitoring.
- If the results fall short, you adjust your plan, make necessary changes, and repeat the PDCA cycle.



A Clear Path to Getting CMMC Compliant

PDCA	CMMC	KEYS
Plan	Identify	NIST 800-171
Do	Remediate	POA&Ms
Check	Verify	SSP
Act	Assess	C3PAO

Framework for Getting CMMC Compliant



Identify *(Plan):*

- Identify the problem = 3rd party NIST 800-171 Risk & Security Assessment
- Set specific targets = Determine your current exposure and desired CMMC level
- Plan how to achieve them = High-level design. Estimated costs. Business buy-in.

Remediate *(Do):*

- Plan how to achieve them (again) = Develop Plans of Action & Milestones (POA&Ms)
- Carry out the planned activities = Execute the POA&Ms and Build Your NIST Security Program

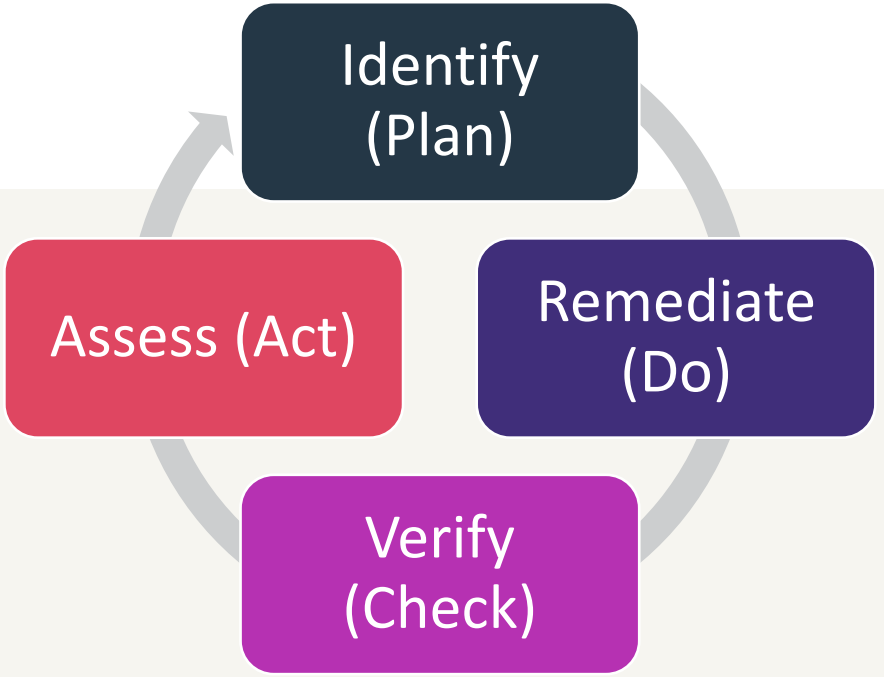
Verify *(Check):*

- Gather data to evaluate the effectiveness of the changes = Perform a follow-up assessment
- Compare the actual to expected outcomes = Build the System Security Plan (SSP) and regenerate SPAR Score

Assess *(Act):*

- Evaluate = Assessment by a certified C3PAO Auditor
- Standardize the improvements, and update processes = Monitor compliance

Identify (Plan)



- **Determine your current exposure**
  - DFARS is effective now
  - Is it mentioned in existing contracts?
  - Where is your CUI today? Who uses it?
  - Who are your customers? Suppliers?
- **Commit to required CMMC level**
  - Based on current and desired business
  - Sets your overall objective
- **Conduct NIST 800-171 Risk & Security Assessment**
  - Not a simple risk or gap assessment. *Use a certified practitioner.*
  - Identify the specified categories of CUI received/developed
  - Map CUI data flow through all Users, Systems, Software and Cloud services
  - Understand initial CMMC compliance report and SPAR score
- **Check the business' appetite**
  - Build a high-level design
  - Estimate costs
  - Socialize with stakeholders

i6 CISO
ELIMINATE REACTIVE

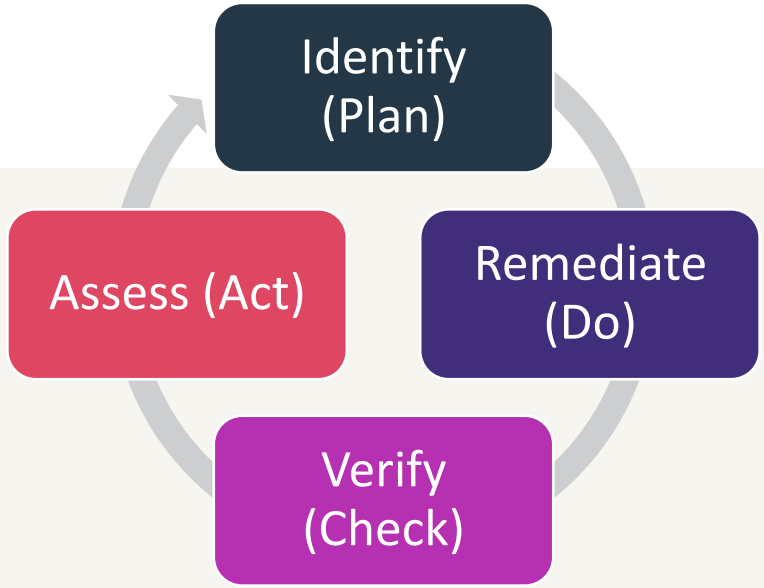
CMMC is about CUI. NIST is about IP.

Critical, Common Areas of Control

Consider People, Process, and Technology for IT and the Business

Estimate the Total Cost of Compliance

Remediate (Do)



- **Align your security program with NIST**
  - NIST-based policies
  - CUI-specific training
  - Identify authorized people (e.g., US Citizens)
  - Governance, Risk, & Compliance Committee
- **Develop Plans of Action & Milestones (POA&Ms)**
  - POA&Ms outline the steps to address and remediate security vulnerabilities, weaknesses, or deficiencies
  - They define the who, what, when, and how
- **Execute the POA&Ms**
  - Executing POA&Ms will take focus, time, and effort
  - POA&Ms should be realistic
  - POA&Ms can be iterative

Deficiency Description				
Milestone #1	Start – End Dates	-	Milestone Status	Not Started
	Planned Milestone			
	Actions Taken			

NIST-Based Security Program is key

Big Remediation Challenges

No business buy-in. No contract awareness.

Understanding how CUI flows through an organization

Inadequate policies, procedures & compliance-related documentation.

High-level System Security Plan (SSP)

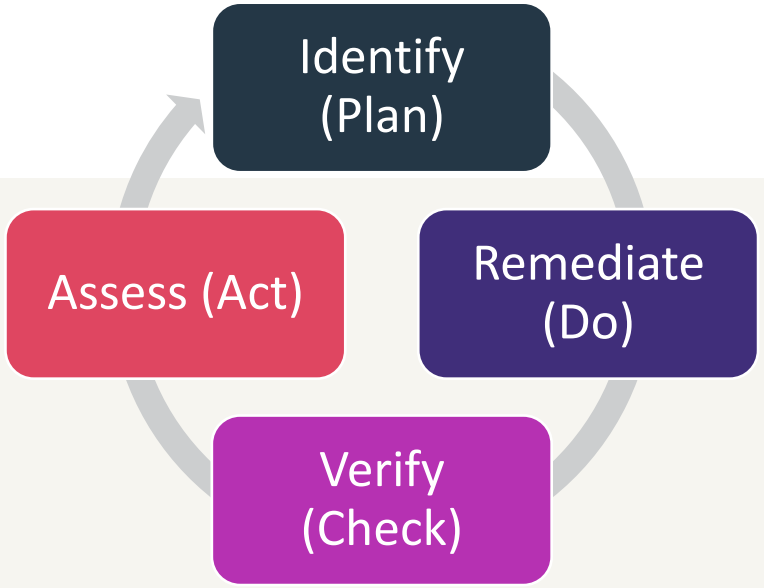
Poor (or missing) Plans of Action and Milestones (POA&M)

Limited security monitoring & incident response capabilities

FIPS-Compliant vs. FIPS-Validated Encryption

FedRAMP-Equivalent vs. FedRAMP-authorized Cloud Services

Verify (Check)



- **Perform a DoD Self-Assessment by a 3rd party**
  - DoD self-assessment helps validate controls and generate the SPAR score
  - Use of an objective, trained, experienced 3rd party is key to avoid internal bias and bring an auditor's perspective
- **Build the System Security Plan (SSP)**
  - An SSP serves as a comprehensive document that outlines the security controls and safeguards implemented in your environment
  - The SSP is the key element of your application for CMMC compliance – auditors will start with the SSP
  - Establish and maintain **sufficient evidence** for your score
- **Regenerate SPAR Score**
  - Update Supplier Performance Risk System (SPRS) score
  - If not 110, return to Identify

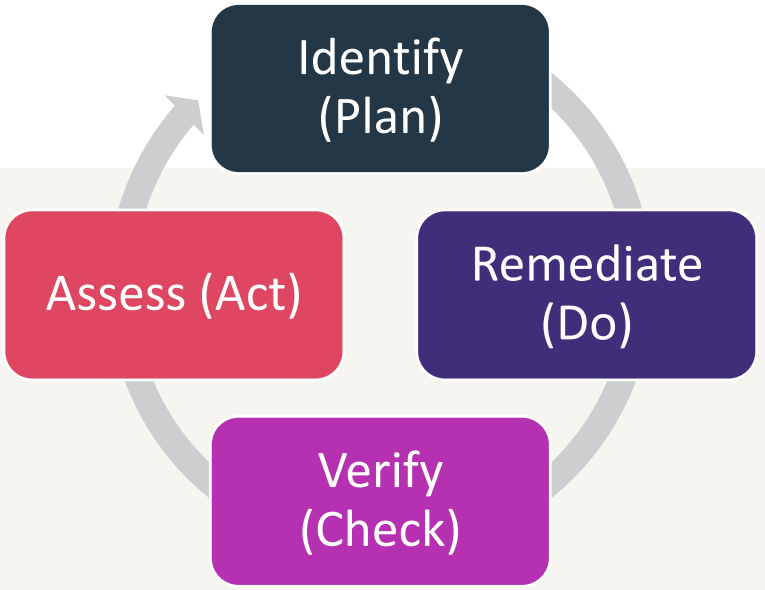
Implementation Status (check all that apply):
☑ Implemented
☐ Partially implemented
☐ Not applicable
☐ Inherited:
☐ Not Implemented

Implementation Details:

Evidence, evidence, evidence

i6 CISO
ELIMINATE REACTIVE

Assess (Act)



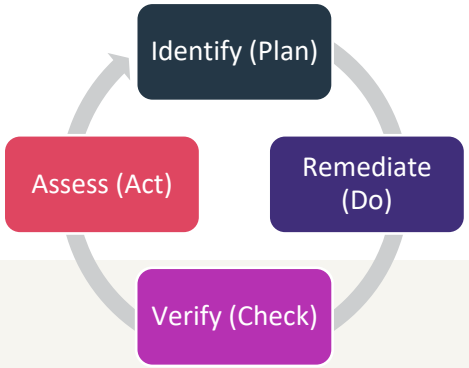
- **Select and Schedule C3PAO**
  - This is an important partner in your journey
  - Spend the time to find a good fit
  - Expect a queue for C3PAOs, especially as the deadline approaches
- **Get the C3PAO Assessment**
  - Showtime!
  - The assess will be a detailed review of SSP and Evidence
- **Monitor and prepare for reassessment**
  - It's critical to understand and communicate that CMMC compliance is not a one-and-done effort
  - Monitoring controls, tracking risks, etc. is a critical element of compliance

Expect long wait times for C3PAOs!

In conclusion…

“Everyone Has A Will To Win But Very Few Have The Will To Prepare To Win.” — Vince Lombardi

CMMC 2023 Summary



CMMC builds on DFARS and NIST 800-171 -- **Rules that you should already be following**

→

The government continues to ramp up regulations and enforcement – **CMMC is real and coming**

→

Closing gaps will require investment in **people, process, and technology**

↓

Passing the assessment gauntlet will require **strong evidence** of people, process, and technology

→

Think about cycles of improvement **– it's not about getting to 110 immediately**

→

Companies that finish early will have an **opportunity to win** business from those that don't

Inversion6

THANK YOU

Jack Nichelson
Chief Information Security Officer