CLARK SCHAEFER CONSULTING

Your CMMC Journey: Navigating Discovery & Assessment

STEP 1: READINESS

By: Serge Kikonda & Ross Patz

Moderator: Carly Devlin

CLARK SCHAEFER CONSULTING

Introduction

SERGE KIKONDA

ROSS PATZ

CARLY DEVLIN

Today's Agenda

CLARK SCHAEFER CONSULTING

1. Overview
2. CMMC Updates
3. Scope Determination
4. Policies & Procedures
5. Control Identification
6. Alliance Building
7. Gap Analysis
8. Preparation for Remediation
9. Q&A

CLARK SCHAEFER
CONSULTING

Overview

Overview

CLARK SCHAEFER CONSULTING

Focus of Step 1 (Readiness):

- Evaluate your organization's security posture.
- Identify vulnerabilities and potential risks that could be exploited by hackers or other malicious entities.
- Perform comprehensive analysis of the network, systems, applications, and other assets to determine the overall level of security.

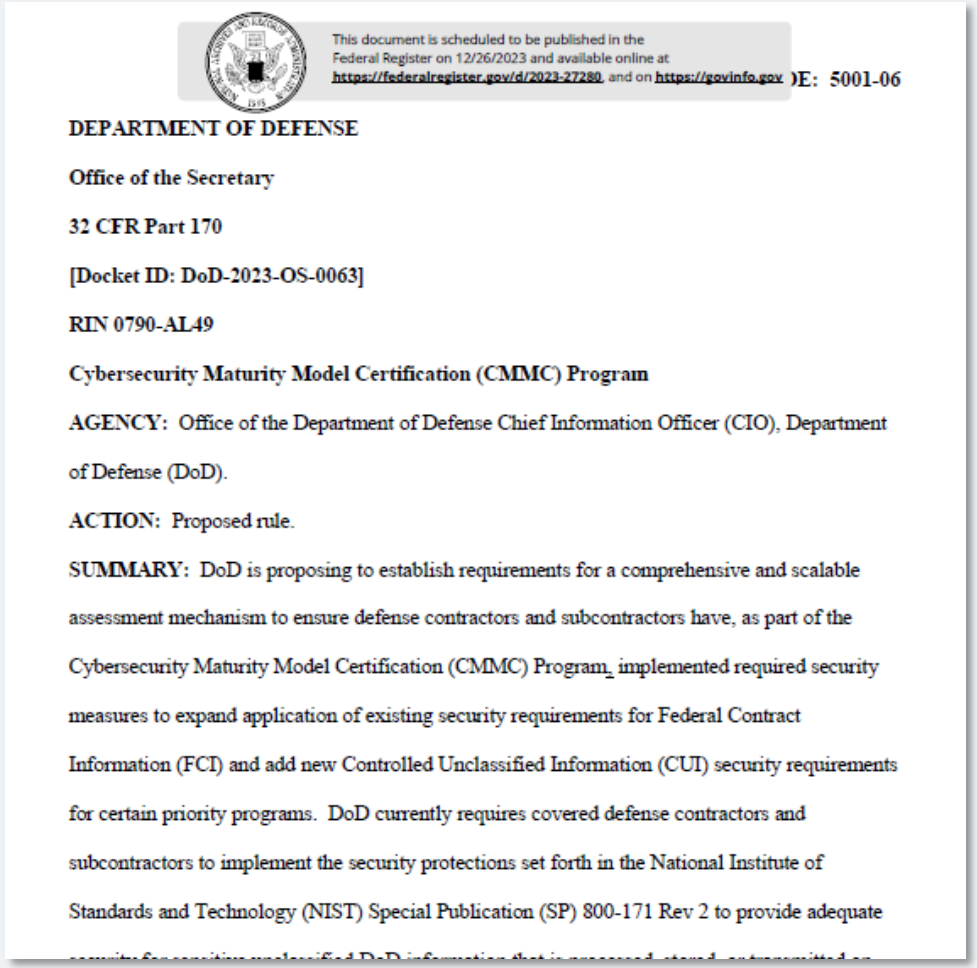
CLARK SCHAEFER CONSULTING

CMMC Updates

CMMC Updates

CLARK SCHAEFER CONSULTING

- **32 CFR for CMMC has been PUBLISHED as a PROPOSED RULE!**
- Outlines CMMC Program
- Defines the general and specific requirements for each level
- Outlines the assessment types required by contract and applicable subcontract



This document is scheduled to be published in the Federal Register on 12/26/2023 and available online at https://federalregister.gov/d/2023-27280, and on https://govinfo.gov

DE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 170

[Docket ID: DoD-2023-OS-0063]

RIN 0790-AL49

Cybersecurity Maturity Model Certification (CMMC) Program

AGENCY: Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD).

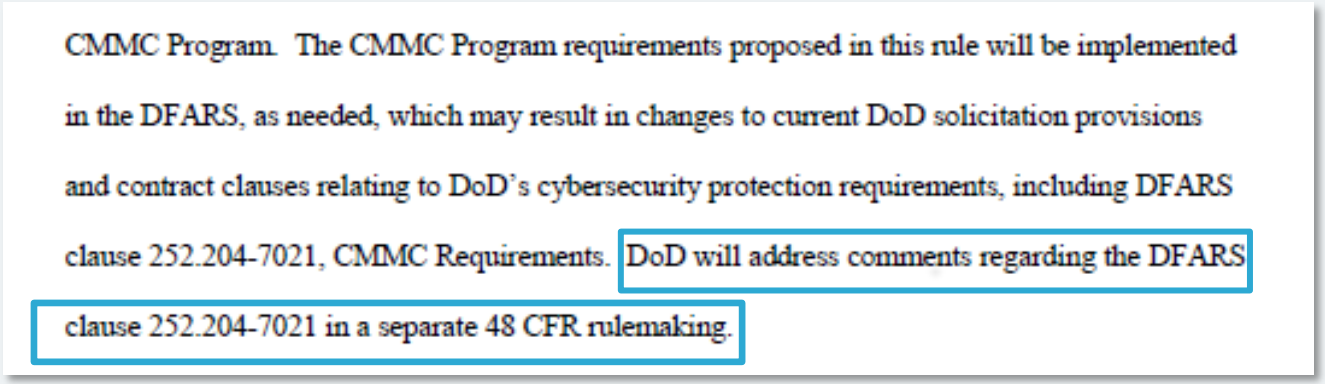
ACTION: Proposed rule.

SUMMARY: DoD is proposing to establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have, as part of the Cybersecurity Maturity Model Certification (CMMC) Program, implemented required security measures to expand application of existing security requirements for Federal Contract Information (FCI) and add new Controlled Unclassified Information (CUI) security requirements for certain priority programs. DoD currently requires covered defense contractors and subcontractors to implement the security protections set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2 to provide adequate

CMMC Updates

CLARK SCHAEFER CONSULTING

- **CMMC becomes effective when the 32 CFR is published as a Final Rule!**
- The phased roll-out of CMMC begins when 48 CFR (CMMC Clause in contracts) is published as a final rule (after rulemaking).



CMMC Program. The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses relating to DoD's cybersecurity protection requirements, including DFARS clause 252.204-7021, CMMC Requirements. DoD will address comments regarding the DFARS clause 252.204-7021 in a separate 48 CFR rulemaking.

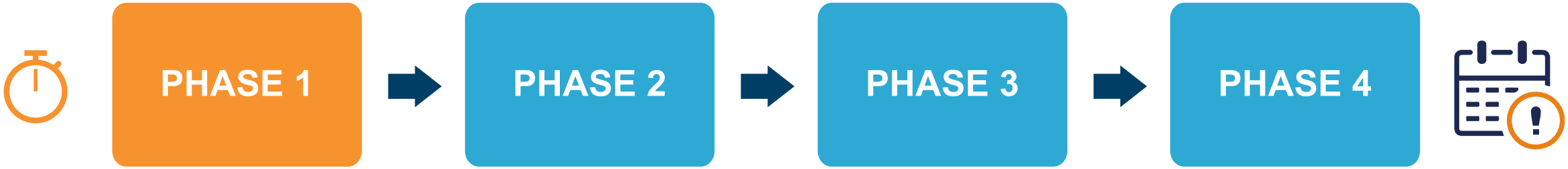
CMMC Timeline

CLARK SCHAEFER CONSULTING

PHASE 1 → PHASE 2 → PHASE 3 → PHASE 4

CMMC Timeline

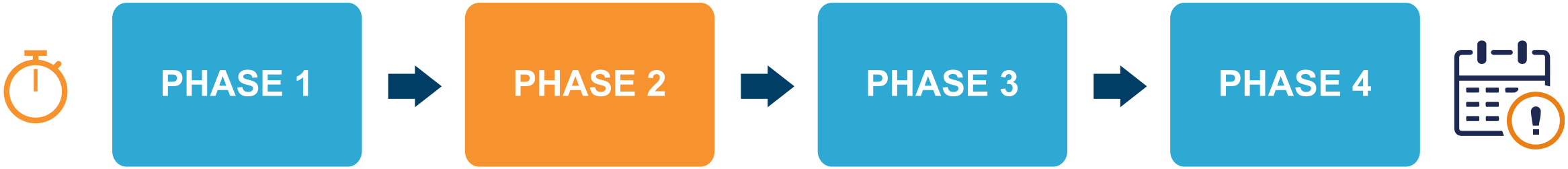
CLARK SCHAEFER CONSULTING



- **Begins on the effective date of 48 CFR!**
- Level 1 and 2 self-assessments requirements in all applicable RFI/RFPs and contracts.

CMMC Timeline

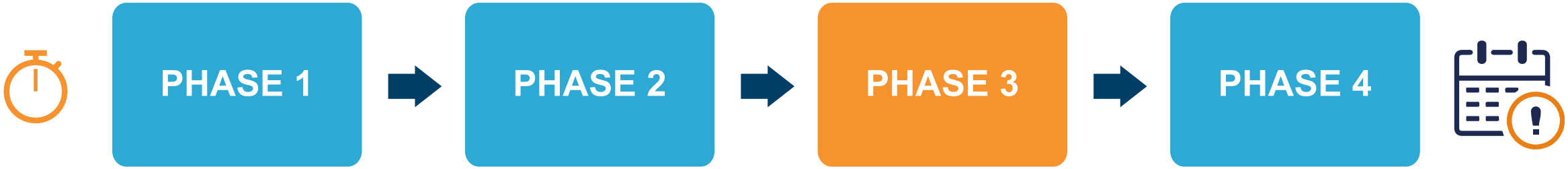
CLARK SCHAEFER CONSULTING



- **Begins 6 months after the start of Phase 1**!
- Level 2 certified assessments requirements in all applicable RFI/RFPs and contracts as a condition of award.

CMMC Timeline

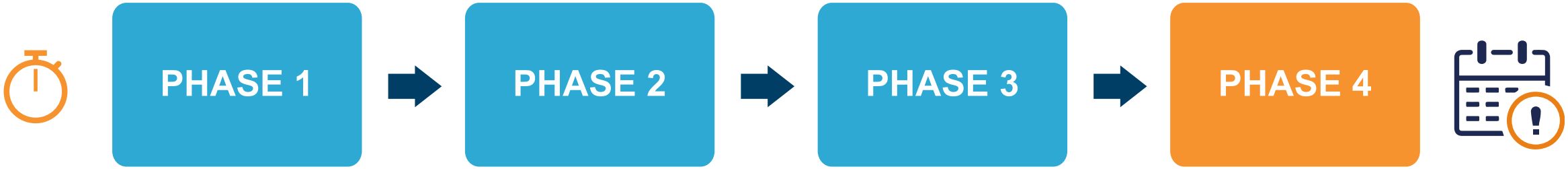
CLARK SCHAEFER CONSULTING



- **Begins 12 months after the start of Phase 2**!
- Level 2 and 3 certified assessments requirements in all applicable RFI/RFPs and contracts as a condition of award.

CMMC Timeline

CLARK SCHAEFER CONSULTING



- **Begins 12 months after the start of Phase 3**!
- CMMC requirements in all applicable RFI/RFPs and contracts prior to the start of Phase 4.

Important To Remember…

CLARK SCHAEFER CONSULTING

Government Program Managers will have discretion to include CMMC requirements or exclude them and rely upon existing DFARS Clause 252.204-7012 requirements, in accordance with DoD policy. As stated in 32 CFR 170.20(a), there is qualified standards acceptance between DCMA DIBCAC High Assessment and CMMC Level 2, which will result in staggering of the dates for new CMMC Level 2 assessments. The implementation period will consist of four (4) phases as set forth in 32 CFR 170.3(e), during which time the Government will include CMMC

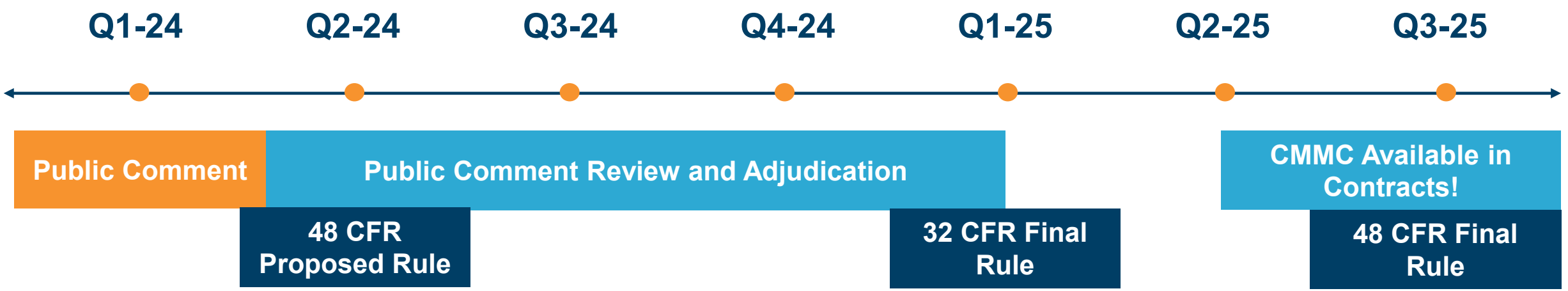
Important To Remember…

CLARK SCHAEFER CONSULTING

assessment services offered by C3PAOs. OSAs may elect to complete a self-assessment or pursue a certification assessment at any time after issuance of the rule, in an effort to distinguish themselves as competitive for efforts that require an ability to adequately protect CUI. For that reason, the number of CMMC assessments for unique entities per level per year may vary

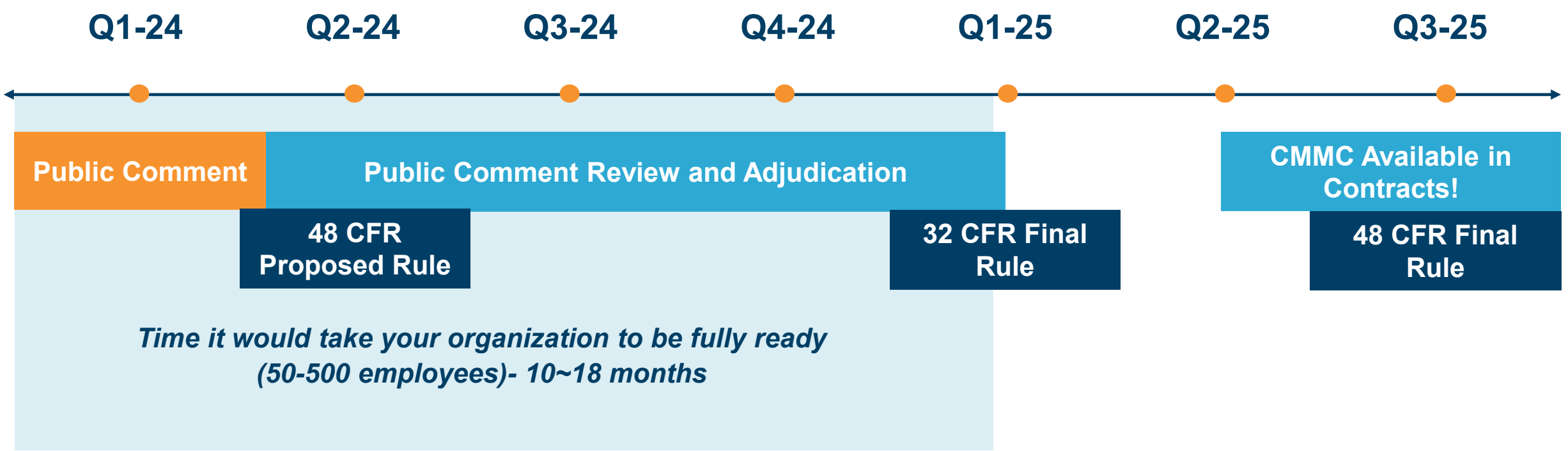
What Does That Mean for You?

CLARK SCHAEFER CONSULTING



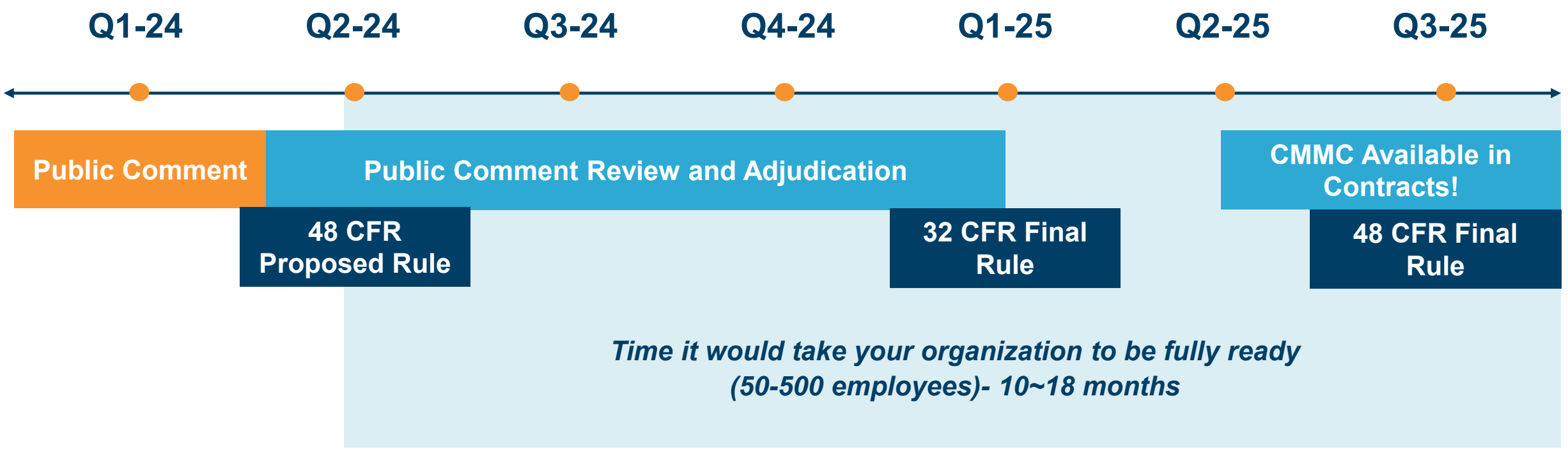
What Does That Mean for You?

CLARK SCHAEFER CONSULTING



What does that mean for you?

CLARK SCHAEFER CONSULTING



CMMC Cost

CLARK SCHAEFER CONSULTING

Assessment Phase ($)	Level 1 Self-Assessment[32]	Level 2 Self-Assessment[32]	Level 2 Certification Assessment	Level 3 Certification Assessment
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,803	$14,426	$20,699	$1,905
Conduct the Assessment	$2,705	$15,542	$76,743	$1,524
Report Assessment Results	$909	$2,851	$2,851	$1,876
Affirmations	$560	*$4,377	*$4,377	*$5,628
Subtotal	$5,977	$37,196	$104,670	$10,933
**POA&M	$0	$0	$0	$1,869
Total	**$5,977**	**$37,196**	**$104,670**	**$12,802**

*Reflects the 3-year cost to match the periodicity.

**Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones.

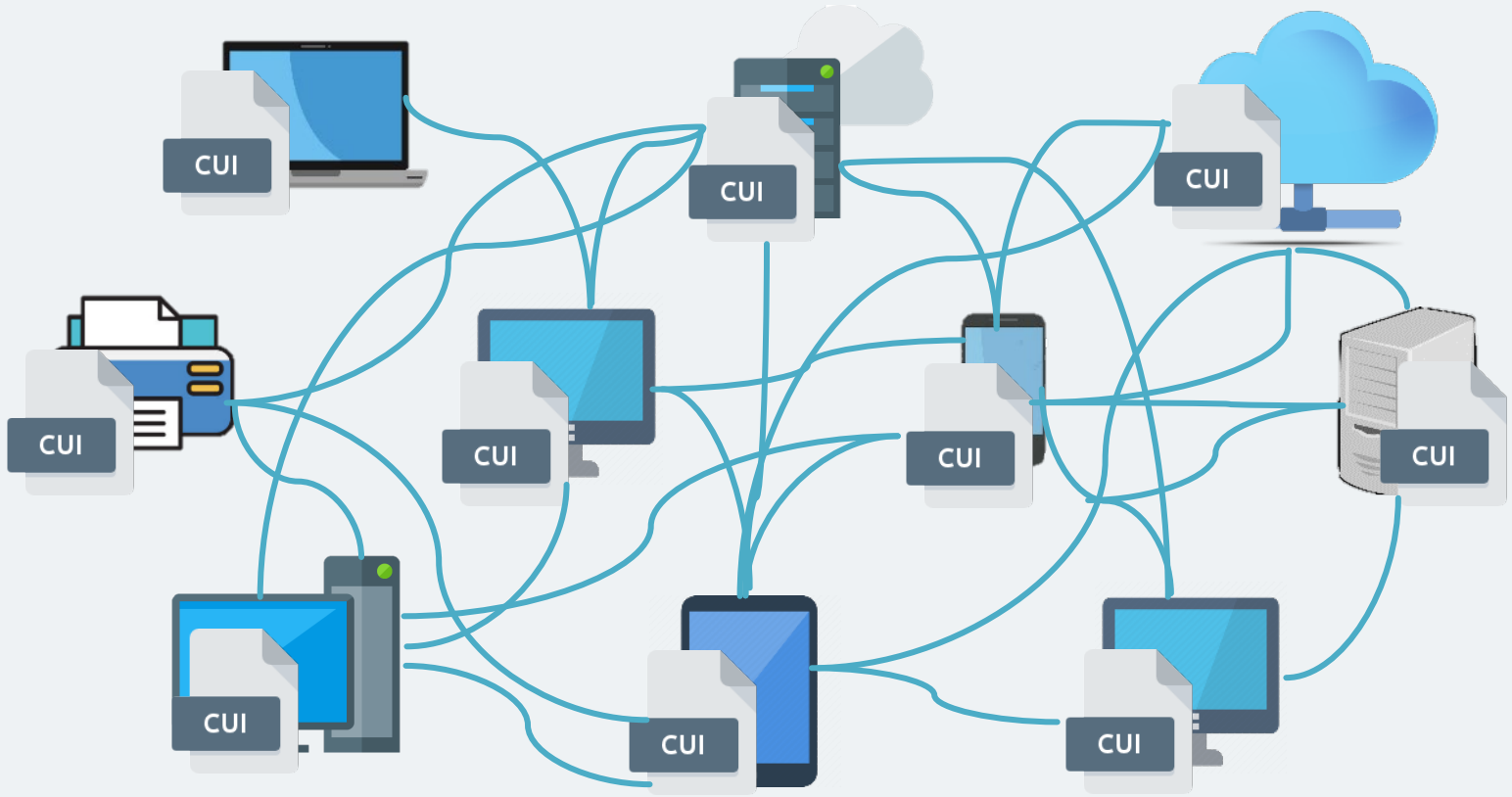
CLARK SCHAEFER CONSULTING

Scope Determination

Assessment Scope

CLARK SCHAEFER CONSULTING

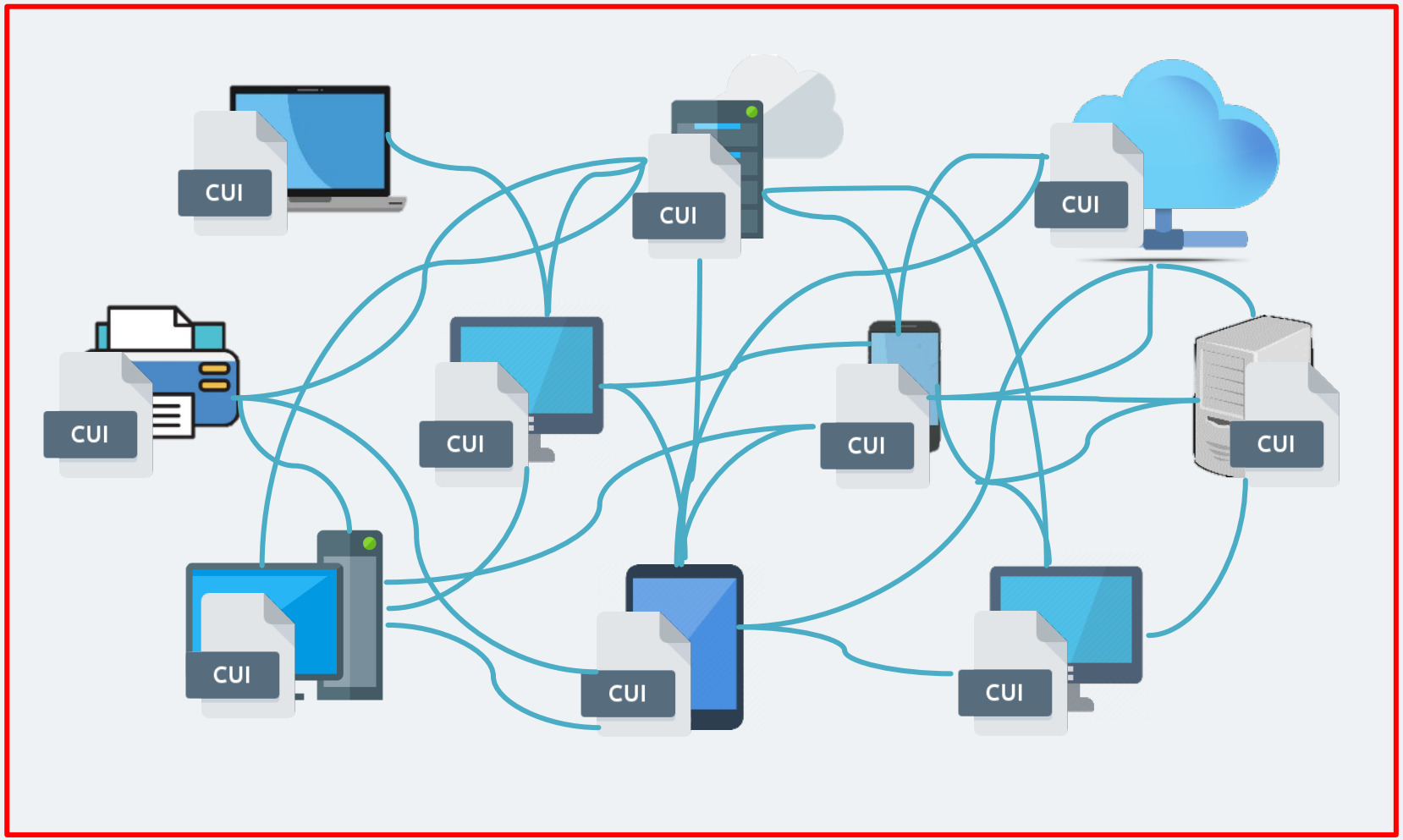
SCENARIO 1



Assessment Scope

CLARK SCHAEFER CONSULTING

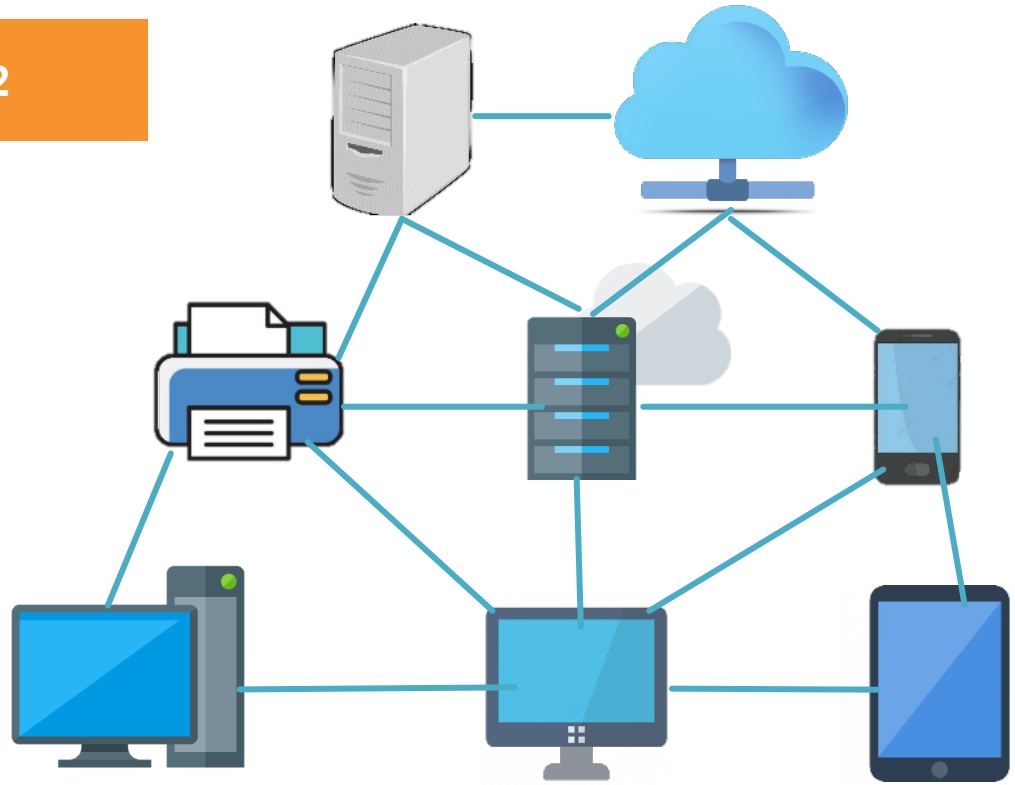
SCENARIO 1

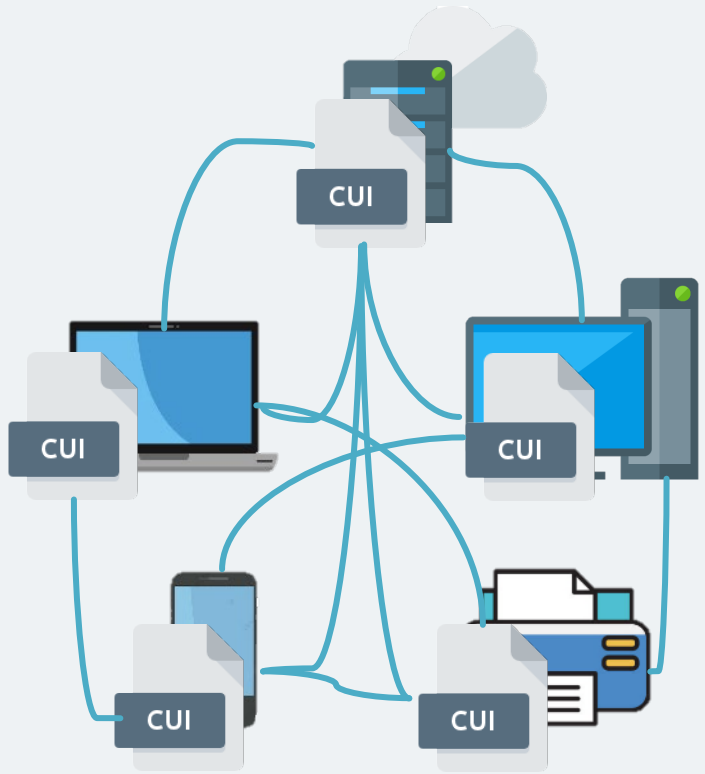


Assessment Scope

CLARK SCHAEFER CONSULTING

SCENARIO 2

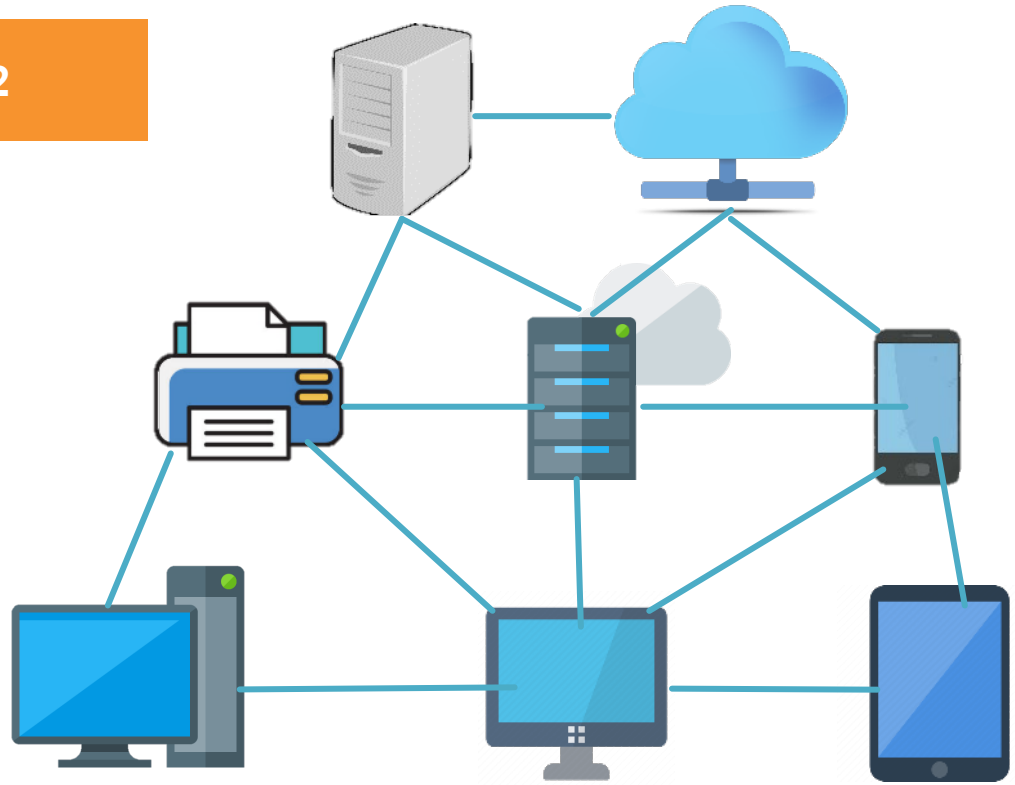


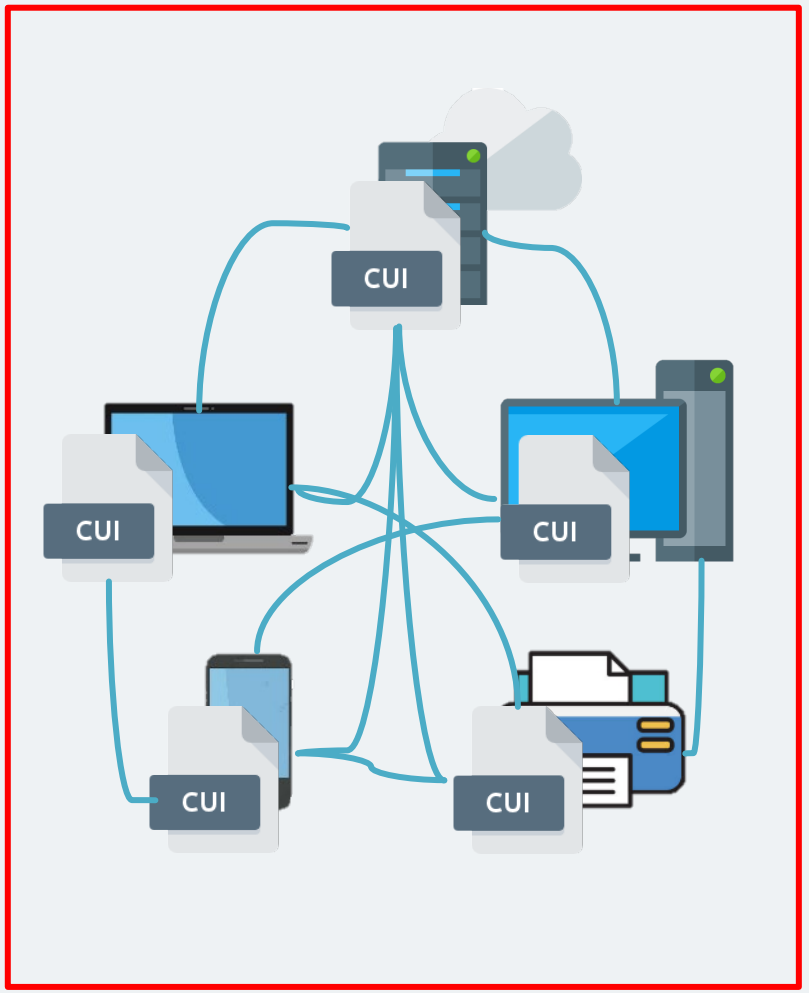


Assessment Scope

CLARK SCHAEFER CONSULTING

SCENARIO 2





CLARK SCHAEFER CONSULTING

Policies & Procedures

Policies & Procedures

CLARK SCHAEFER CONSULTING

The Importance of Policies & Procedures:

- Increase compliance
- Enable consistent processes & structures
- Provide a roadmap for day-to-day operations
- Keep operations consistent and controlled
- Ensure that rules, standards, and controls are clearly outlined

Policies & Procedures

CLARK SCHAEFER CONSULTING

The Difference Between Policies & Procedures:

- A **policy** is a predetermined course of action. It is the link between an organization's vision/values and day-to-day operations.

- A **procedure** explains a specific action plan for carrying out a policy. They eliminate common misunderstandings by identifying job responsibilities and establish boundaries for those jobs.

Policies & Procedures

CLARK SCHAEFER CONSULTING

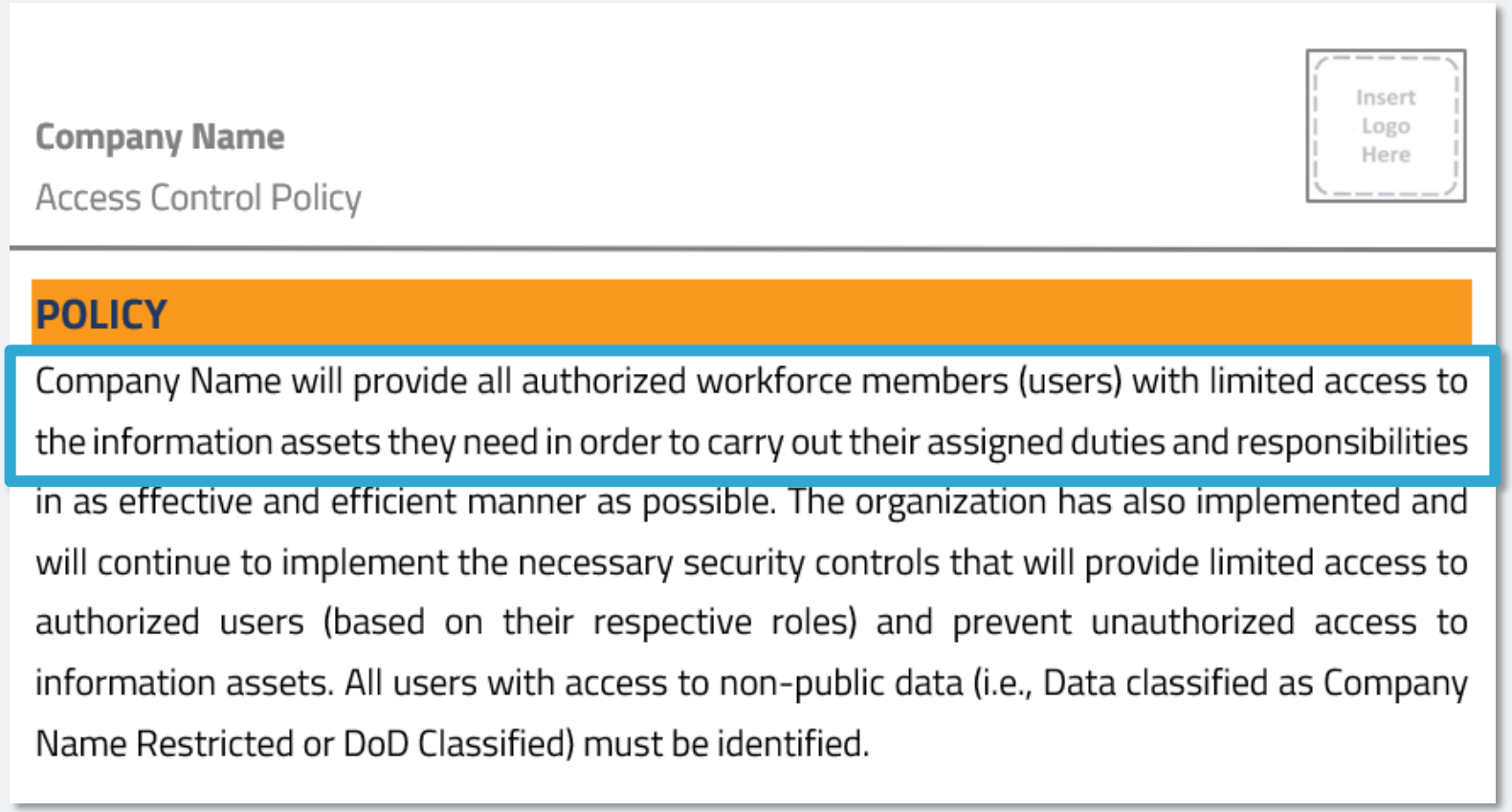
Example:

- Access Control Policy

Policies & Procedures

CLARK SCHAEFER CONSULTING

A **policy** is a predetermined course of action.



Company Name

Access Control Policy

Insert Logo Here

POLICY

Company Name will provide all authorized workforce members (users) with limited access to the information assets they need in order to carry out their assigned duties and responsibilities in as effective and efficient manner as possible. The organization has also implemented and will continue to implement the necessary security controls that will provide limited access to authorized users (based on their respective roles) and prevent unauthorized access to information assets. All users with access to non-public data (i.e., Data classified as Company Name Restricted or DoD Classified) must be identified.

Policies & Procedures

CLARK SCHAEFER CONSULTING

A **procedure** explains a specific action plan for carrying out a policy.

PROCEDURES

Privileged Access

Access to and use of privileged accounts (e.g., Local administrator, domain administrator, root, etc.) will be restricted, controlled, and not provided by default. Authorization for the use of such accounts requires written approval from the **IT Administrator**. Authorized users must submit the request to their immediate supervisor first. The former must determine if such access is necessary, before the request is submitted to the **IT Administrator** for final approval.

CLARK SCHAEFER CONSULTING

Control Identification

Identifying Controls

CLARK SCHAEFER CONSULTING

- Use the most up-to-date version of the CMMC Assessment Guide (based on NIST 800-171 R2)

CMMC Assessment Guide
Level 2

Identifying Controls

CLARK SCHAEFER CONSULTING

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Identifying Controls

CLARK SCHAEFER CONSULTING

Current Implementation

[a] The means of limiting unsuccessful logon attempts is defined.
Organizational systems are configured to limit the number of invalid login attempts. Devices are secured with a password to prevent unauthorized access. Authorized users are allowed up to **3 consecutive unsuccessful attempts** before their account is disabled and locked for **30 minutes**.

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTE

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Identifying Controls

CLARK SCHAEFER CONSULTING

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Identifying Controls

CLARK SCHAEFER CONSULTING

Key Questions:

- Do you have a System Security Plan (SSP)?
- Are the controls in place documented in the SSP?
- Are the controls in place operating effectively?
- Are the controls in place reviewed periodically?
- Are the controls in place tested?

CLARK SCHAEFER CONSULTING

Alliance Building

Identify Your Team

CLARK SCHAEFER CONSULTING

Who Does the Organization Work or Partner With?

- Third-Party Vendors (e.g., SOC)
- Managed Service Providers (MSP)
- Managed Security Service Providers (MSSP)
- Other organizations?

Identify Your Team

CLARK SCHAEFER CONSULTING

Key Things To Remember...

All these organizations can only do so much.

You are responsible for holding them accountable.

Their failures may become your failures.

Identify Your Team

CLARK SCHAEFER CONSULTING

Registered Provider Organization (RPO)

- Can help as little or as much as you need.
- Provide pre-assessment consulting services to government contractors and other Organizations Seeking Certification (OSCs) and/or assist during assessments in the event a finding is uncovered.

Identify Your Team

CLARK SCHAEFER CONSULTING

Key Questions:

- Are the people you are working with fully aware of their roles and responsibilities?
- Are there clearly written agreements and expectations?
- Are there periodic reviews to ensure that people are doing what they are expected to do?
- What are the consequences if services are not being performed as intended/agreed upon?

CLARK SCHAEFER CONSULTING

Gap Analysis

Identifying Gaps

CLARK SCHAEFER CONSULTING

How To Identify Your Gaps

- Identify the areas of weakness in your security controls.
- Document them in a Plan of Action and Milestones (POA&M).
- This is an opportunity to strengthen or “harden” your environment through carefully planned improvements.

Identifying Gaps

CLARK SCHAEFER CONSULTING

POA&M

- A POA&M is a document that helps an organization prioritize and manage cybersecurity risks effectively.
- It outlines the steps an organization needs to take to address identified vulnerabilities or weaknesses in its environment.

Identifying Gaps

CLARK SCHAEFER CONSULTING

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Identifying Gaps

CLARK SCHAEFER CONSULTING

Current Implementation

[a] The means of limiting unsuccessful logon attempts is defined.
Organizational systems are configured to limit the number of invalid login attempts. Devices are secured with a password to prevent unauthorized access. Authorized users are allowed up to **3 consecutive unsuccessful attempts** before their account is disabled and locked for **30 minutes**.

AC.L2-3.1.8 – UNSUCCESSFUL LOGO

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Identifying Gaps

CLARK SCHAEFER CONSULTING

404 Not Found

AC.L2-3.1.8 – Unsuccessful Logon Atter

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

Identifying Gaps

CLARK SCHAEFER CONSULTING

Control Family	Control Section	CMMC Practice	Assessment Objectives	Implementation Status	Control Owner	Evidence gathered (e.g., Screenshot)?	Comments
Access Control (AC)	3.1.	AC.L2- 3.1.8	[a] the means of limiting unsuccessful logon attempts is defined	FULLY MET	Bruce Wayne	Refer to SSP	
Access Control (AC)	3.1.	AC.L2- 3.1.8	[b] the defined means of limiting unsuccessful logon attempts is implemented	NOT MET	Tony Stark	Screenshot from Microsoft AD needed	Control needs to be implemented. Then Screenshot must be gathered.

Identify Your Gaps

CLARK SCHAEFER CONSULTING

Key Questions

- Does your organization have a POA&M?
- Are all the gaps & vulnerabilities documented?
- Are the control owners identified?
- Are gap remediation action steps identified?
- Has a remediation plan/timeline been established?

Preparation for Remediation

Preparing For Step 2 (Remediation)

CLARK SCHAEFER CONSULTING

8 Questions To Prepare for the Remediation Step

1. Have you fully completed Step 1 (Readiness)?
2. Have you documented all identified gaps & vulnerabilities?
3. Have you identified control owners?
4. Have you identified what you need for remediation (e.g., resources, funding, new tools, additional staff, etc.)?
5. Have you determined how long remediation could potentially take?
6. Have you established priorities (i.e., what needs to be addressed first)?
7. Do you know when remediation is expected to start?
8. Are you aware of the potential impact on business operations (e.g., interruptions, negative user experience, etc.)?

Next Steps & Resource Pointers

CLARK SCHAEFER CONSULTING

1. **Understand how CMMC applies to your organization**
   - Check out our free survey to help with this: https://www.cshco.com/cmmc-survey/

2. **Start planning your roadmap, conduct a gap analysis, and remediate**
   - Clark Schaefer Consulting is a CMMC Registered Provider Organization (RPO) and can help with CMMC readiness, remediation work, or ongoing maintenance work.

If you have questions, need more information, or are ready to start your CMMC journey, check out our CMMC info page https://www.cshco.com/cmmc or contact us at cmmc@clarkschaefer.com.

Future CMMC Information

CLARK SCHAEFER CONSULTING

- Continued webinar series on CMMC by Clark Schaefer Consulting
- Keep an eye out for email communications!
- Clark Schaefer Consulting will be sending out resources to help with your CMMC journey.

CLARK SCHAEFER CONSULTING

Thank you!

SERGE KIKONDA

ROSS PATZ

CARLY DEVLIN