

A guide to navigating CMMC compliance for small and medium-sized businesses

7 Steps to CMMC with Microsoft Partner, Summit 7



Executive Remarks

Richard Wakeman



Chief Architect
Aerospace & Defense
Microsoft

<https://www.linkedin.com/in/wakeman>

Topics



What is CMMC?



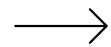
Introducing Summit 7



7 Steps to CMMC Overview



Where to start?



Next Steps!

What is CMMC?

Cybersecurity Maturity Model Certification (CMMC)

WHAT IS CMMC?
A US DoD unified standard for implementing cybersecurity establishing three certification levels reflecting the maturity and reliability of a company's cybersecurity infrastructure to safeguard sensitive government information.

WHY CMMC?
The **certification** will provide assurance that certified organizations can be trusted to store **Federal Contract Information (FCI)** and **Controlled Unclassified Information (CUI)**
"Trust but Verify"

WHEN IMPLEMENTED?
CMMC 2.0 is back in the rule making process and is anticipated to become law in 2023-2024. CMMC Levels 2 assessments are rolling out beginning in 2022 with Joint Surveillance alongside the US DoD's DIBCAC Program.

WHO DOES IT AFFECT?
All US DoD contractors including the **Defense Industrial Base (DIB)** with over 350,00 companies in the supply chain. A CMMC "flow-down" requirement ensures all sub-contractors are compliant as required.

HOW TO CMMC?
DoD **Contractors** may undergo an independent assessment from a CMMC **Certified 3rd-Party Assessment Organization (C3PAO)** to obtain the certification at CMMC Level 2.

WHO WILL MANAGE CMMC?
Cyber Accreditation Board (AB). The **Cyber-AB** is a non-profit organization sanctioned by the US DoD and is responsible for quality and oversight of the independent assessments by C3PAOs.



Cybersecurity Maturity Model Certification Overview

How is CMMC managed?

The Cyber Accreditation Body (AB) is responsible for quality and oversight of the independent assessments for CMMC Level 2 facilitated by C3PAOs.

The **certification** provides assurance that an organization can be trusted to store **Controlled Unclassified Information (CUI)** and **Federal Contract Information (FCI)**.

How do I get CMMC Certified?

US DoD contractors may undergo **an independent assessment from a CMMC Certified 3rd Party Assessor Organization (C3PAO)** to obtain a certification at CMMC Level 2.

CMMC compliance needs to be maintained and **re-assessed every 3 years**.

What's next?

CMMC is currently being replicated **outside of DoD** and may apply to future contracts from DHS, DOE, NASA. It is also expected to expand to the **international supply chain** of these agencies.

The Microsoft Trusted Cloud

We build our Trusted Cloud on four foundational principles



Security

We build our services from the ground up to help safeguard your data



Privacy

Our policies and processes help keep your data private and, in your control,



Compliance

We provide industry-verified conformity with global standards











Transparency

We make our policies and practices clear and accessible to everyone

Learn more: [Microsoft Trust Center](#)

Microsoft has one of the largest compliance portfolios in the industry

GLOBAL

 ISO 27001	 ISO 27018	 ISO 27017	 SOC 1 Type 2	 SOC 2 Type 2	 CSA STAR Self-Assessment	 CSA CCM	 WCAG 2.0 AA	 ISO 20000-1 ¹	 CIS Benchmark
--	--	--	---	--	--	--	---	---	---

US GOV

 FedRAMP High	 DoD DISA SRG Level 2 ²	 DoD DISA SRG Level 4 ²	 DoD DISA SRG Level 5 ²	 NIST SP 800-171 ² SP 800-53	 FIPS 140-2	 Section 508	 ITAR ²	 CJIS ²	 IRS 1075 ²	 DFARS ²	 CMMC ²
--	---	---	--	---	---	--	--	--	--	---	--

INDUSTRY

 GLBA	 FFIEC	 Japan FISC	 HIPAA / HITECH Act	 HITRUST Self- assessment	 FDA GxP 21 CFR Part 11	 FERPA	 Netherlands NEN 7510
---	--	--	---	---	---	--	--

REGIONAL

 Argentina PDPA	 Australia IRAP/CCSL	 EU Model Clauses	 EU GDPR	 EU EN 301 549	 EU ENISA IAF	 EU-US Privacy Shield	 UK G-Cloud	 Germany IDW PS 951	 Germany C5 ³	 Germany IT Grundschutz workbook ³
 Canada Privacy Laws	 Netherlands BIR 2012	 Spain ENS	 New Zealand GCIO	 Singapore MTCS	 China DJCP ¹	 China GB 18030 ¹	 China TRUCS ¹	 Japan My Number Act	 Japan CS Mark Gold	

Classified as Microsoft Confidential
¹ Only for Office 365 operated by 21 Vianet | ² Applies to US Govt. GCC, GCC High, or DoD clouds | ³ Only for Office 365 Germany

Microsoft as the platform of choice for CMMC 2.0



Microsoft is a....

Cloud Service Provider
Systems Integrator
Defense Contractor

Mission Cloud

Commercial
US Government (GCC & GCC High)
US Government Secret
US Government Top Secret

Complete Cloud

Productivity
Infrastructure
Security Suite
DevOps & SecOps

We build our Trusted Cloud on four foundational principles



Security



Privacy



Compliance



Transparency



Licensing



Migration & Implementation



MSP & MSSP



Daniel Akridge

DIRECTOR OF ENGAGEMENT,
SUMMIT 7



Sam Stiles

VP OF MARKETING,
SUMMIT 7

 THE 7 STEPS TO
CMMC *Step by Step*
COMPLIANCE
FOR SMALL-MEDIUM BUSINESSES

WITH DANIEL AKRIDGE & SAM STILES

Meet Big Acronym

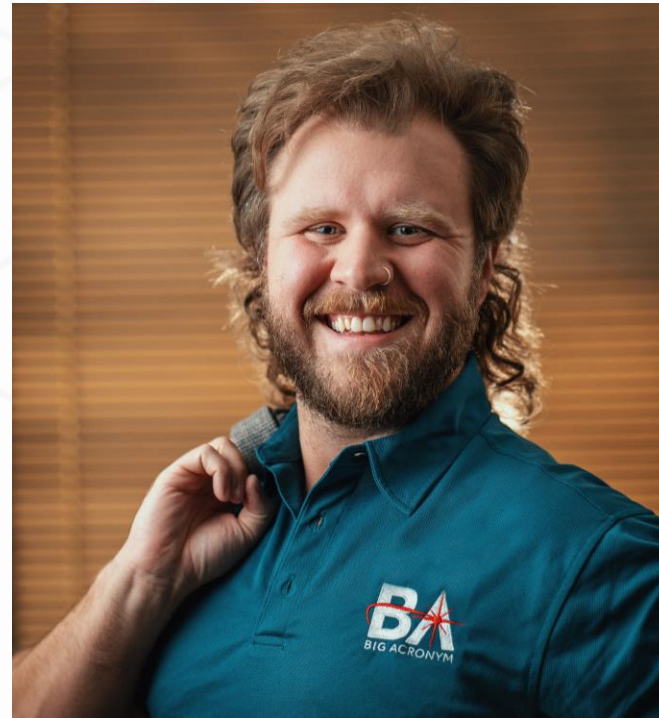


50 Person Manufacturing Company

Uses a Managed Service Provider

Has Controlled Unclassified Information (CUI) Requirements

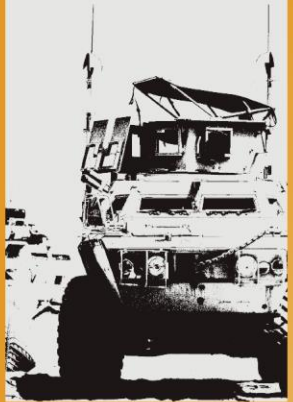
Has Export Control data handling requirements (ITAR)



7 STEPS TO CMMC COMPLIANCE

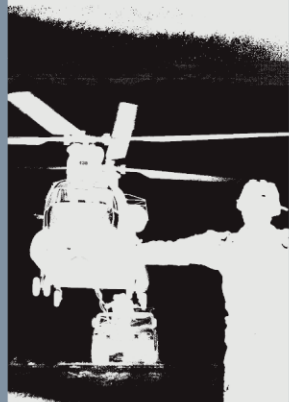
Step One

Identify Your
CMMC Level



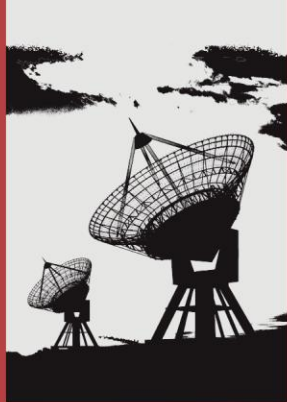
Step Two

Identify Assets
for CMMC



Step Three

Choose A
Technical
Design for
CMMC



Step Four

Implement
Microsoft
Government
for CMMC



Step Five

Find A
Managed
Service
Provider for
CMMC



Step Six

Prepare For
A CMMC
Assessment

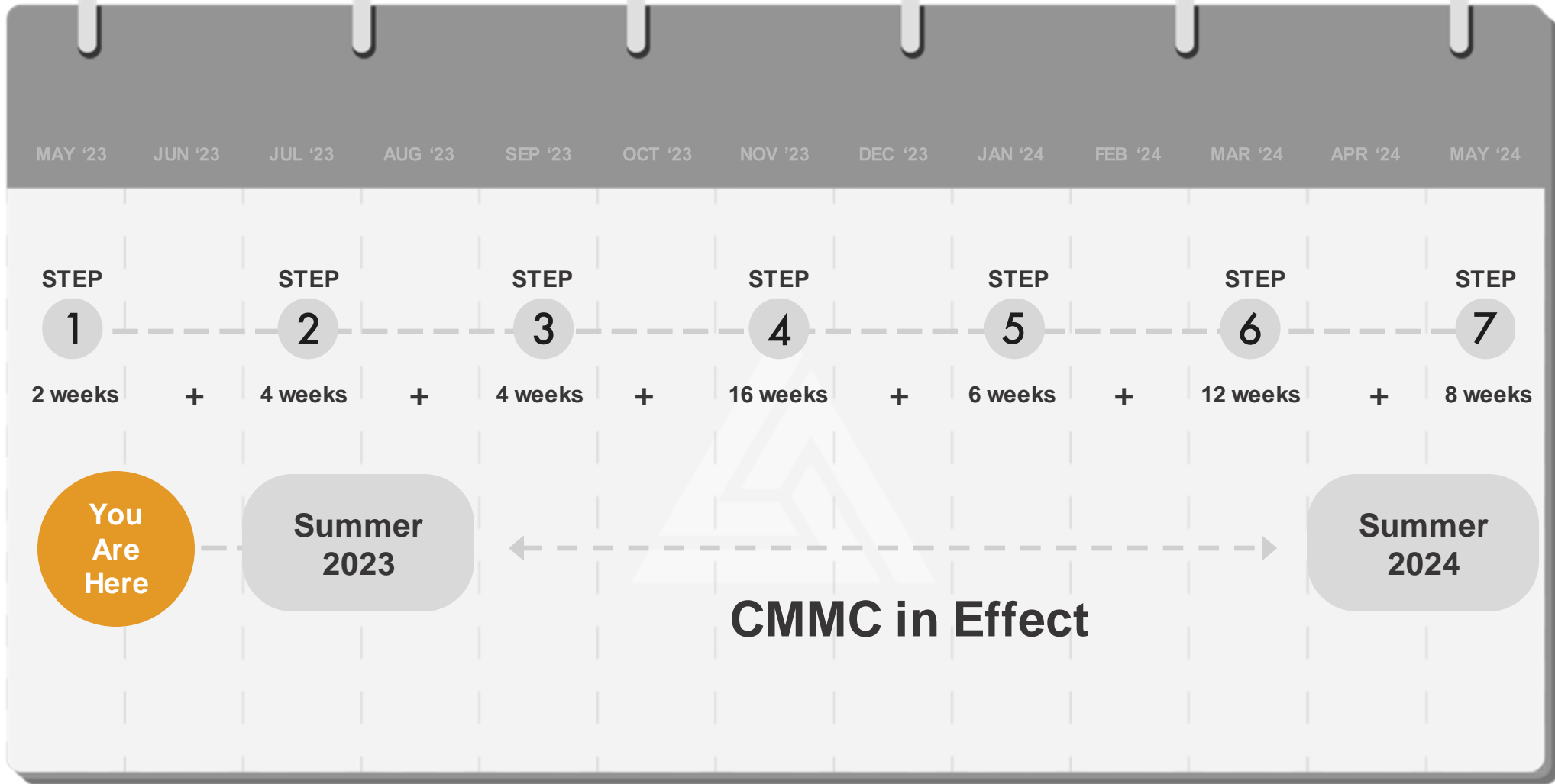


Step Seven

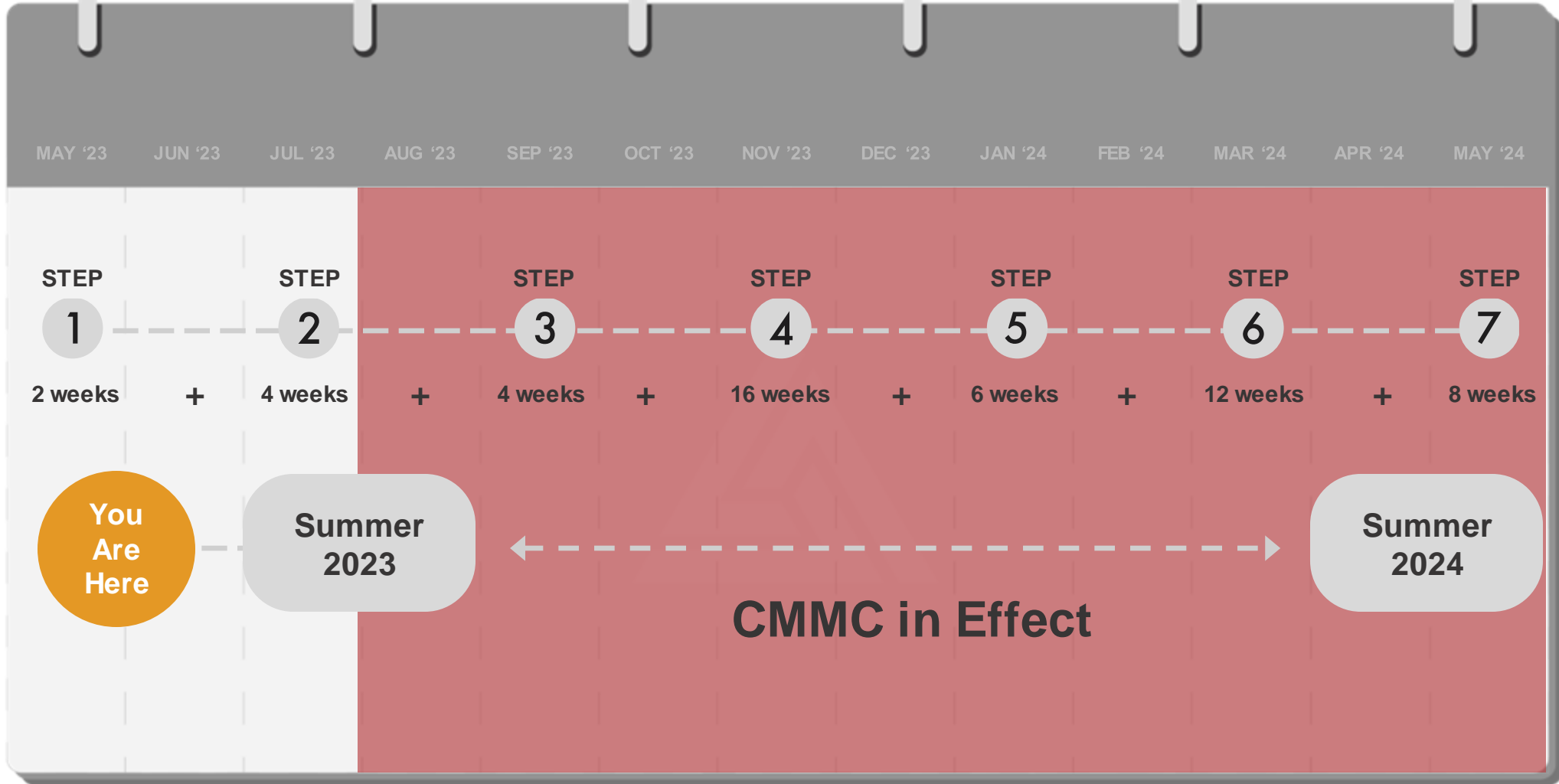
Complete A
CMMC
Assessment



7 Steps Versus CMMC Timeline



7 Steps Versus CMMC Timeline



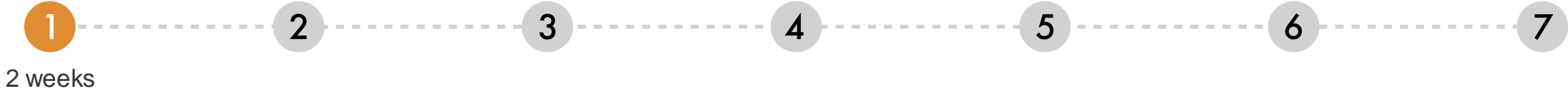
Step One

Identify Your CMMC Level



Step 1: Identify Your CMMC Level

CMMC Level	Existing Contract Requirements	Sensitive Data Types
Level 1	FAR 52.204-21	FCI
Level 2	DFARS 252.204-7012	CUI
Level 3	DFARS 252.204-7012 + DIBCAC High Assessment	CUI/Critical CUI



Step Two

Identify Assets for CMMC



Step 2: Identify Assets for CMMC



ERP



2 weeks



6 weeks



Step 2: Identify Assets for CMMC



ERP



Controlled Unclassified Information



What Is A CUI Asset?

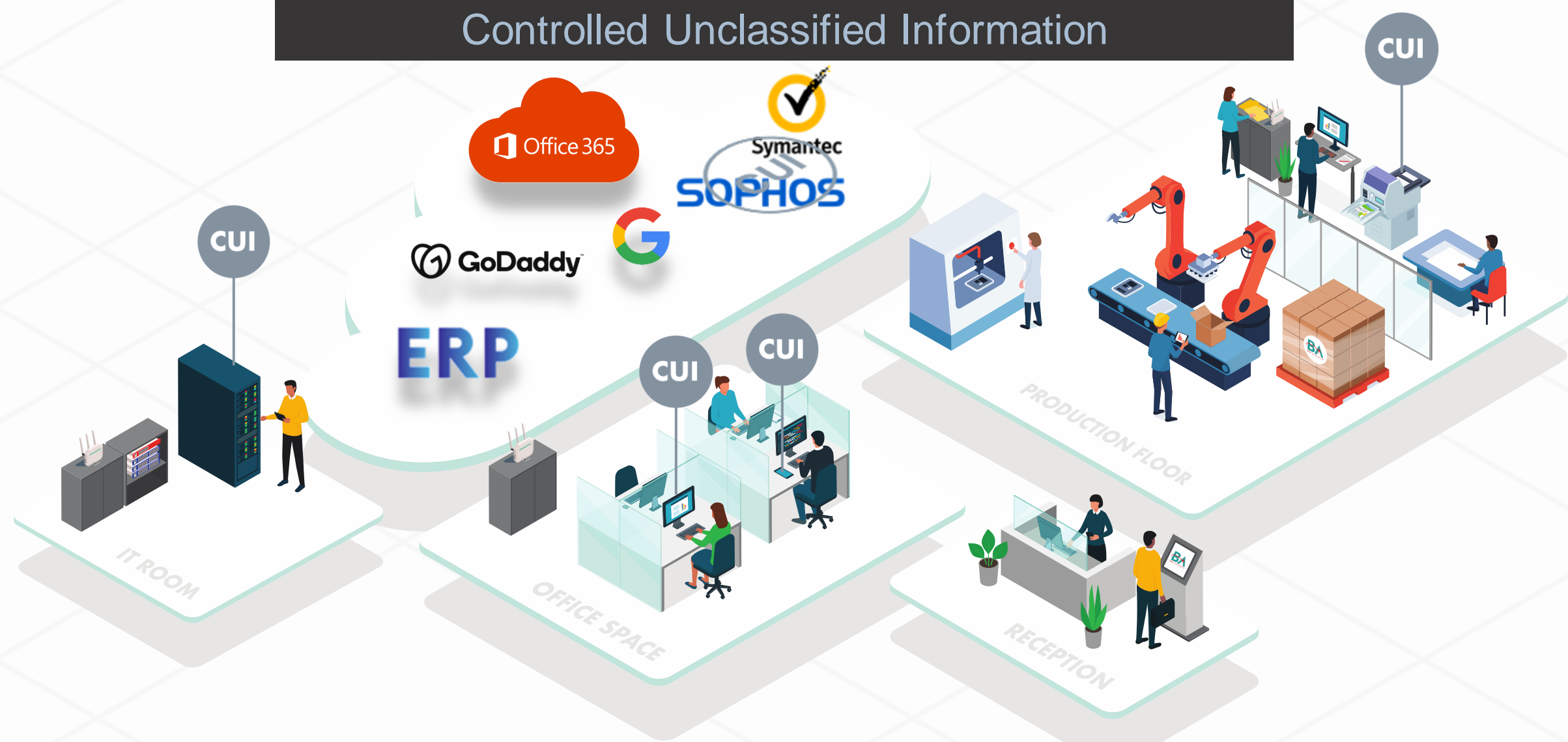
Assets that process, store, or transmit CUI

Requirements:

- Document in Asset Inventory
- Document in SSP
- Document in Network Diagram
- Apply CMMC L2 Practices



Controlled Unclassified Information



Security Protection Asset

SOPHOS



Symantec

SPA

What Is A Security Protection Asset?

Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether these assets process, store, or transmit CUI.

Requirements:

- Document in Asset Inventory
- Document in SSP
- Document in Network Diagram
- Apply CMMC L2 Practices



2 weeks

2

6 weeks

3

4

5

6

7

Security Protection Asset



Contractor Risk Managed Asset



What Is A Contractor Risk Managed Asset?

Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place.

Assets are not required to be physically or logically separated from CUI assets

Requirements:

Document in Asset Inventory

Document in SSP

Document in Network Diagram

If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks



Contractor Risk Managed Asset



SOPHOS



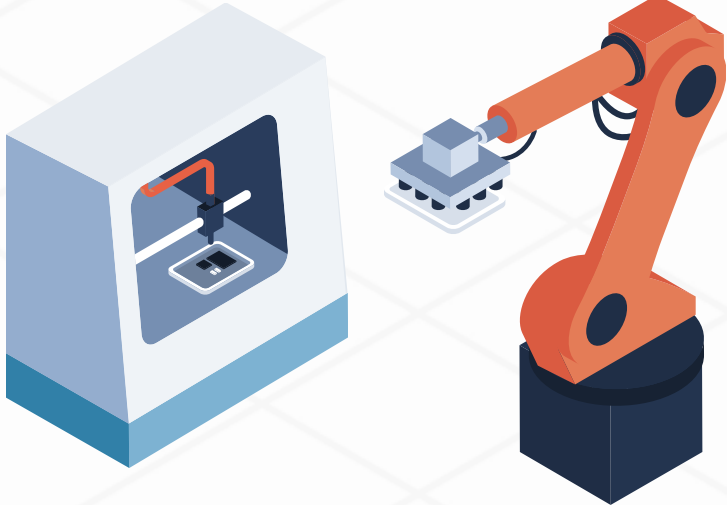
ERP



2 weeks

6 weeks

Specialized Asset



What Is A Specialized Asset?

Assets that may or may not process, store, or transmit CUI

Assets include Government Property, IoT, Operational Technology, Restricted Info Systems, and Test Equipment

Requirements:

- Document in Asset Inventory
- Document in SSP
- Document in Network Diagram



Specialized Asset



SOPHOS



ERP



PRODUCTION FLOOR



IT ROOM



OFFICE SPACE



RECEPTION



2 weeks



6 weeks



Step Three

Choose A Technical Design for CMMC



Step 3: Choose A Technical Design for CMMC



“All In”

CUI Enclave



Step 3: Choose A Technical Design for CMMC



SOPHOS



ERP



2 weeks



4 weeks



4 weeks



Step 3: Choose A Technical Design for CMMC

Do you know where all your CUI data lives?

Do you have data residency/sovereignty requirements outside of the US?

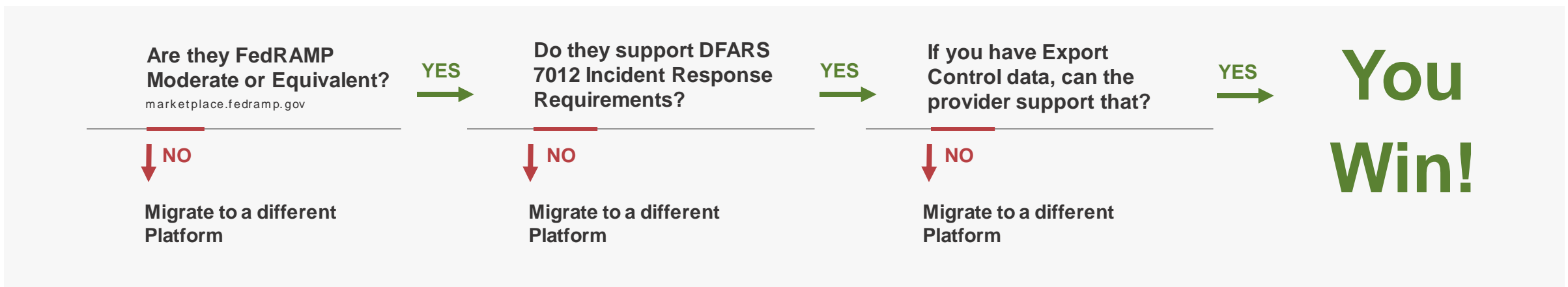
Do 15-20% or more of your employees need access to CUI?

What method is going to be easier and more cost effective to manage?



Step 3: Choose A Technical Design for CMMC

What are the requirements for my Cloud Providers that store, process, or transmit CUI?



Step 3: Choose A Technical Design for CMMC

CMMC Level 1 (FCI)	CMMC Level 1-2 (FCI + Basic CUI)	CMMC Level 2-3 (FCI + Basic CUI + Specified CUI)
M365 Commercial Azure Commercial	M365 GCC Azure Commercial	M365 GCC High Azure Government
NO DFARS 7012	DFARS 7012	DFARS 7012 + ITAR / EAR / NOFORN



Step 3: Choose A Technical Design for CMMC

Meets Future Business Compliance Requirements

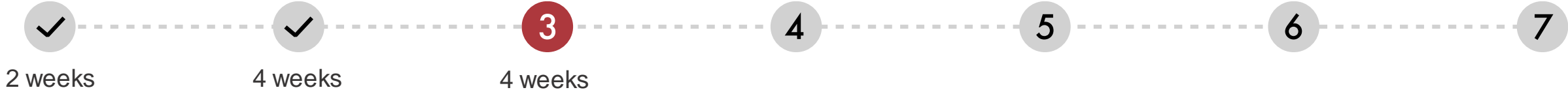
Start here if you know it will be needed in the future. If not a 2nd Implementation and Migration is required

Meets Existing Business Compliance Requirements & Export Control

CMMC Level 2-3
(Basic + Specified CUI)

**M365 GCC High
Azure Government**

DFARS 7012
+ ITAR / EAR / NOFORN

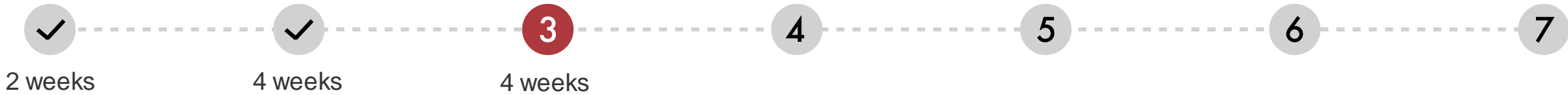


Step 3: Choose A Technical Design for CMMC



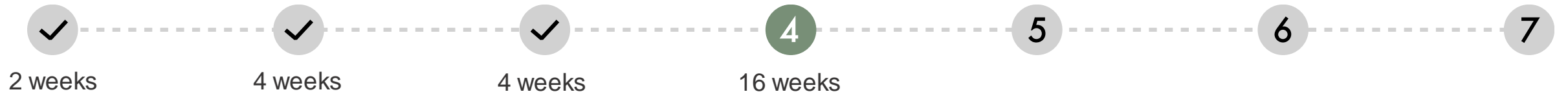
“All In”

CUI Enclave



Step Four


Implement Microsoft Government for CMMC



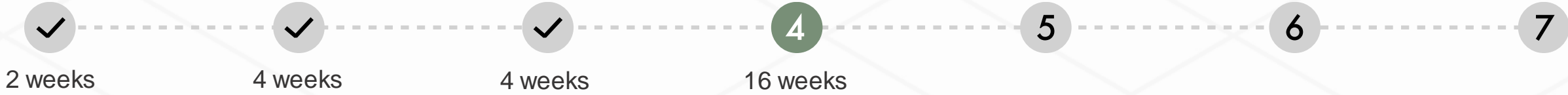
Step 4: Implement Microsoft Government for CMMC



 **Corporate User with Company Device**

 **Frontline Collaboration User / Onsite Contractor**
(SHARED DEVICE OR BYOD MOBILE)

OR

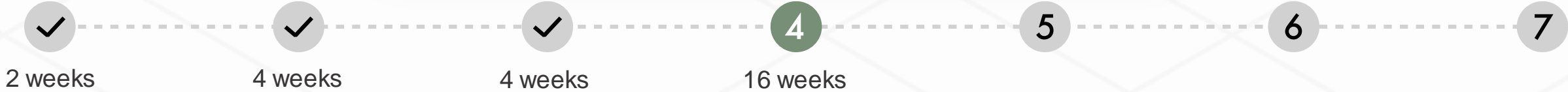
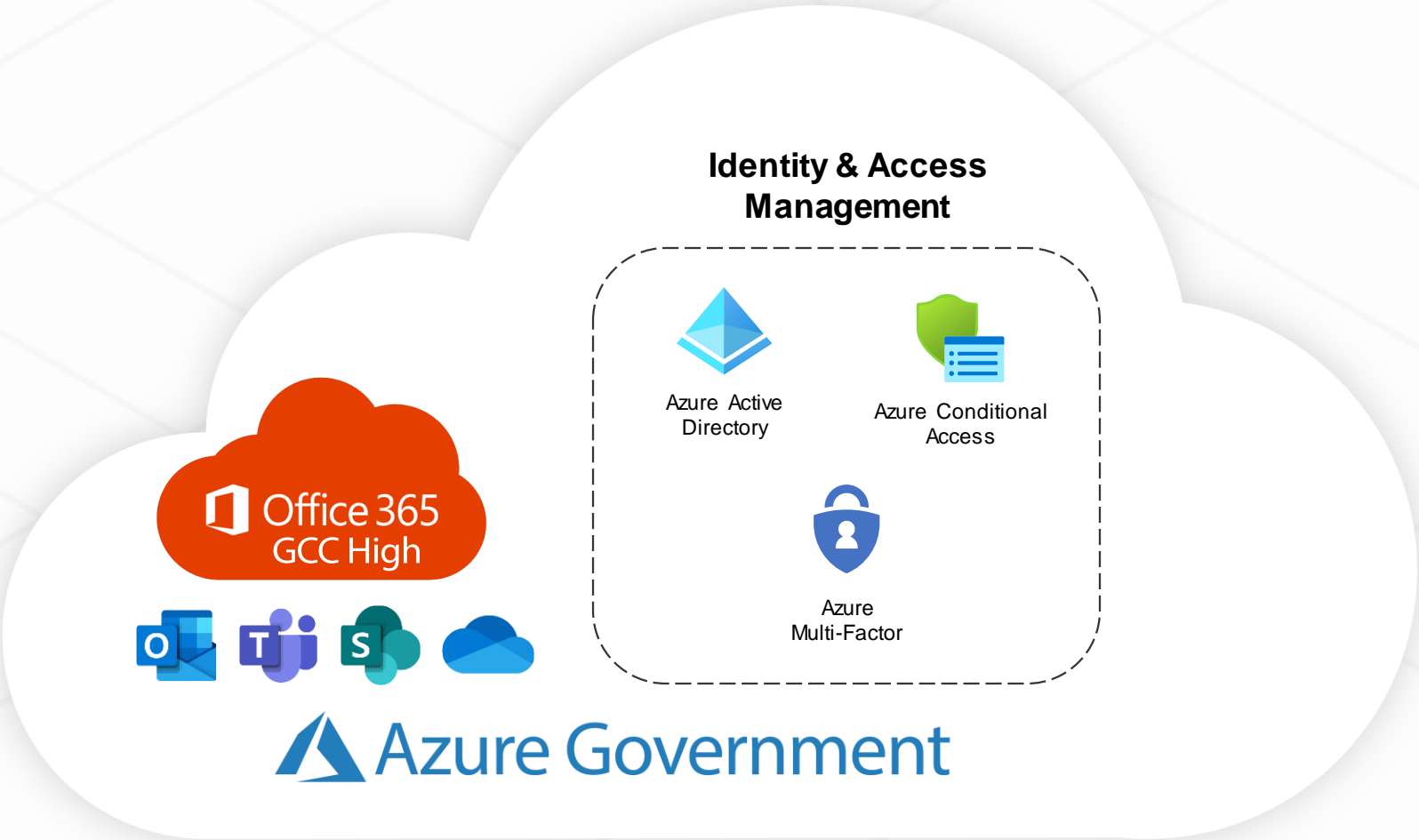


Step 4: Implement Microsoft Government for CMMC

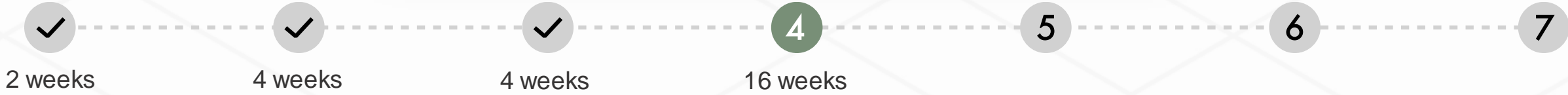
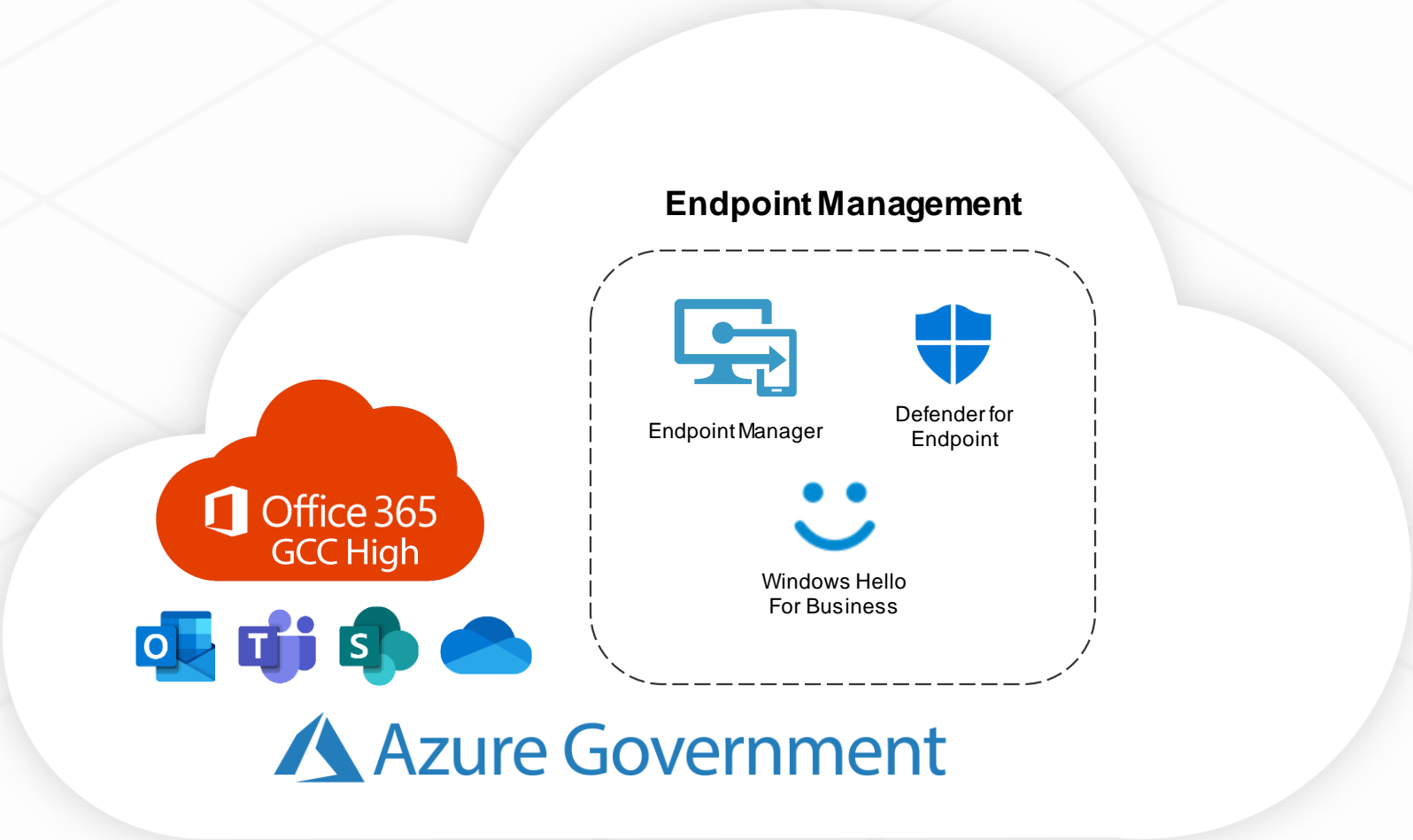


- ✓ 2 weeks
- ✓ 4 weeks
- ✓ 4 weeks
- 4 16 weeks
- 5
- 6
- 7

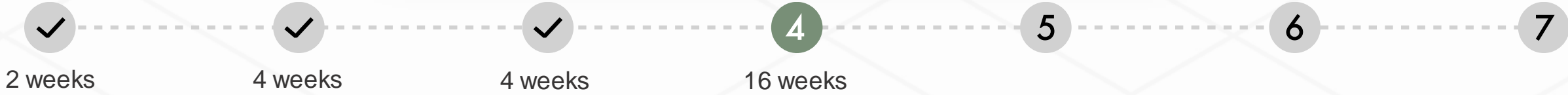
Step 4: Implement Microsoft Government for CMMC



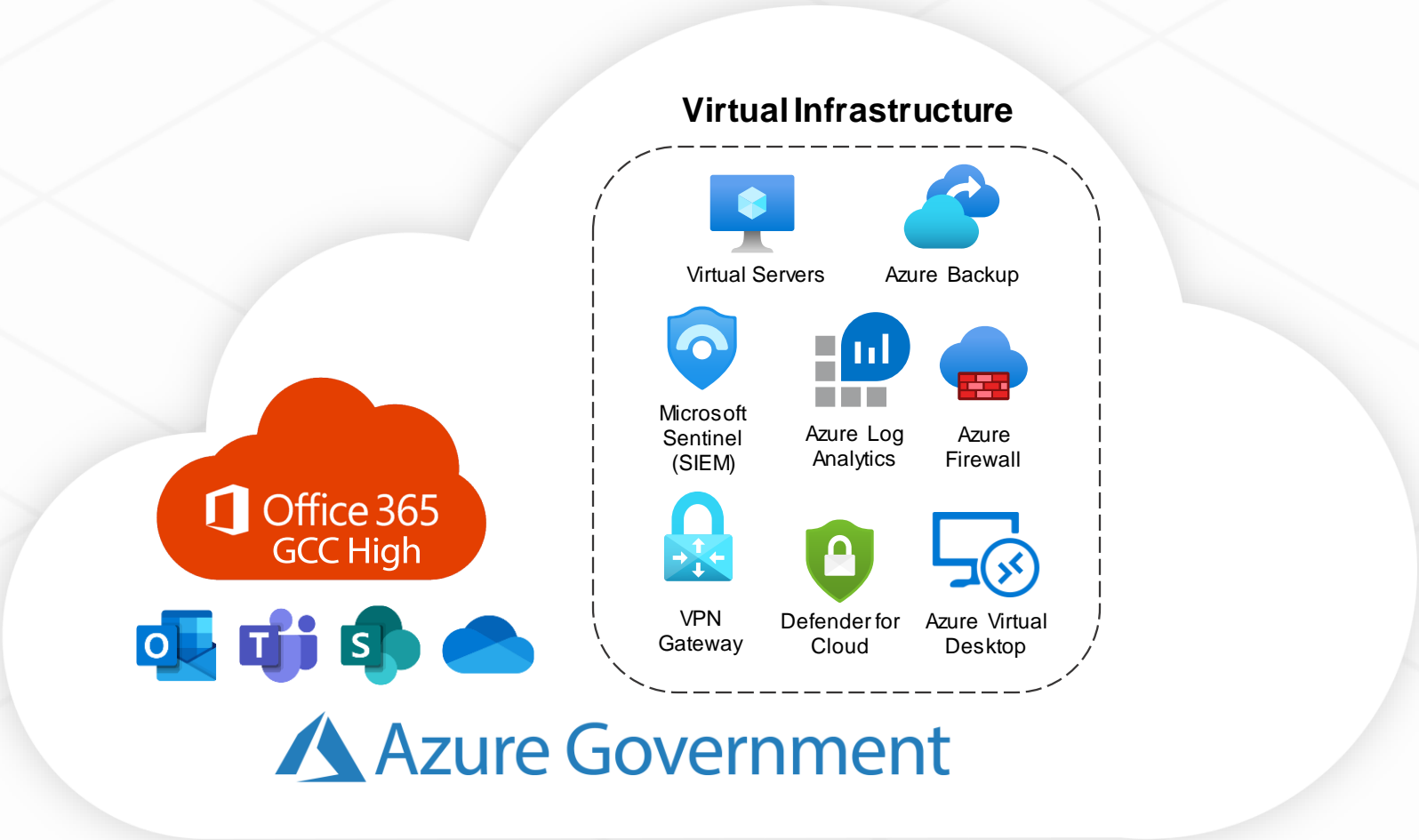
Step 4: Implement Microsoft Government for CMMC



Step 4: Implement Microsoft Government for CMMC



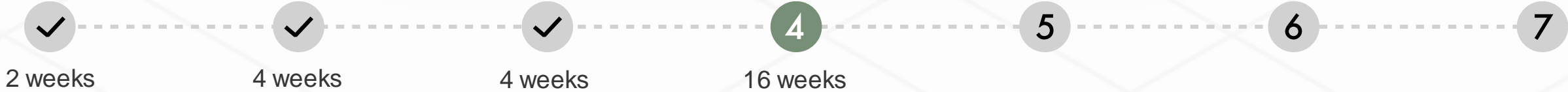
Step 4: Implement Microsoft Government for CMMC



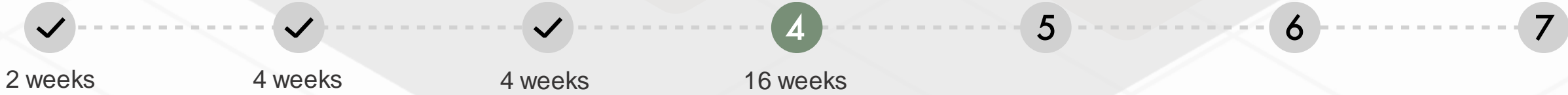
Timeline showing progress through 7 steps:

- Step 1: 2 weeks (checked)
- Step 2: 4 weeks (checked)
- Step 3: 4 weeks (checked)
- Step 4: 16 weeks (highlighted)
- Step 5: 5 weeks
- Step 6: 6 weeks
- Step 7: 7 weeks

Step 4: Implement Microsoft Government for CMMC

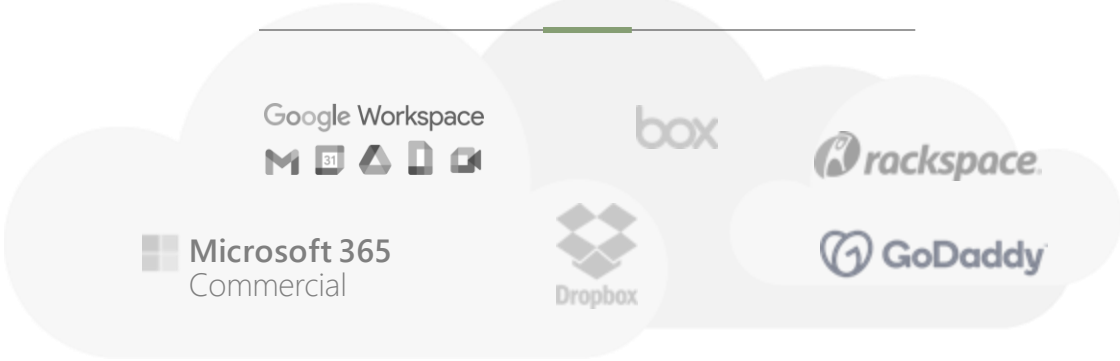


Step 4: Implement Microsoft Government for CMMC

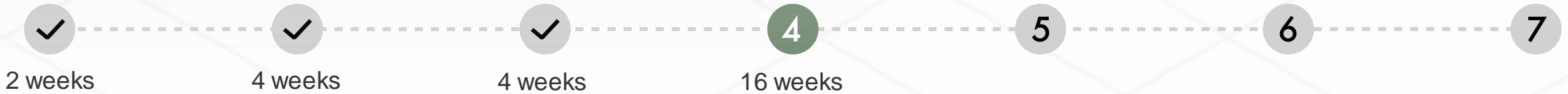


Step 4: Implement Microsoft Government for CMMC

COMMERCIAL CLOUDS



ON PREM SYSTEMS



CONTINUE THE 7 STEPS TO CMMC COMPLIANCE

VIST

summit7.us/steps-to-cmmc-compliance

Step Five

Find A
Managed
Service
Provider for
CMMC



Step Six

Prepare For
A CMMC
Assessment



Step Seven

Complete A
CMMC
Assessment



Questions?

Contact Us



256.585.6868



cmmc@summit7.us



summit7.us