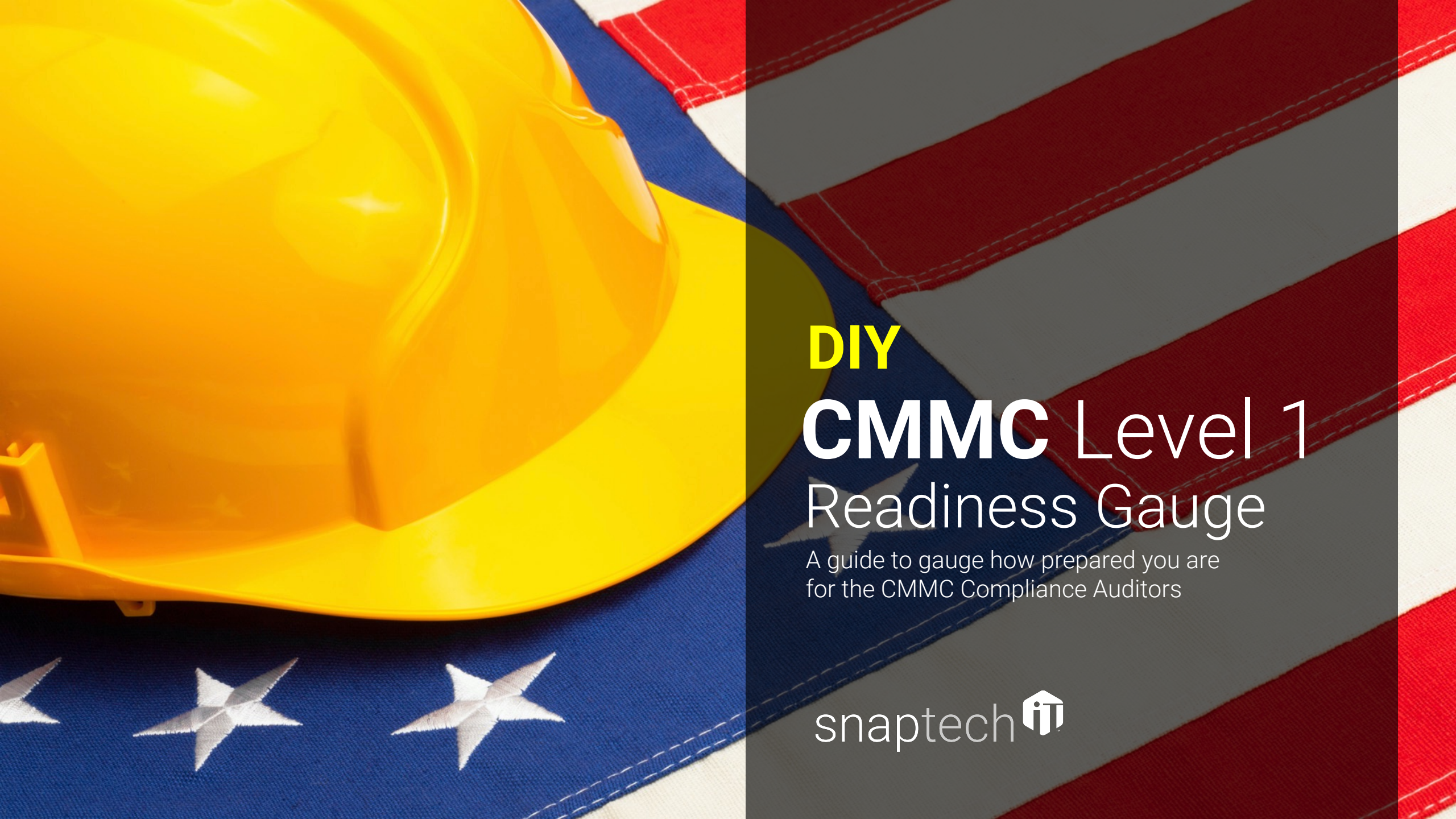


DIY
CMMC Level 1 Readiness Gauge

A guide to gauge how prepared you are for the CMMC Compliance Auditors

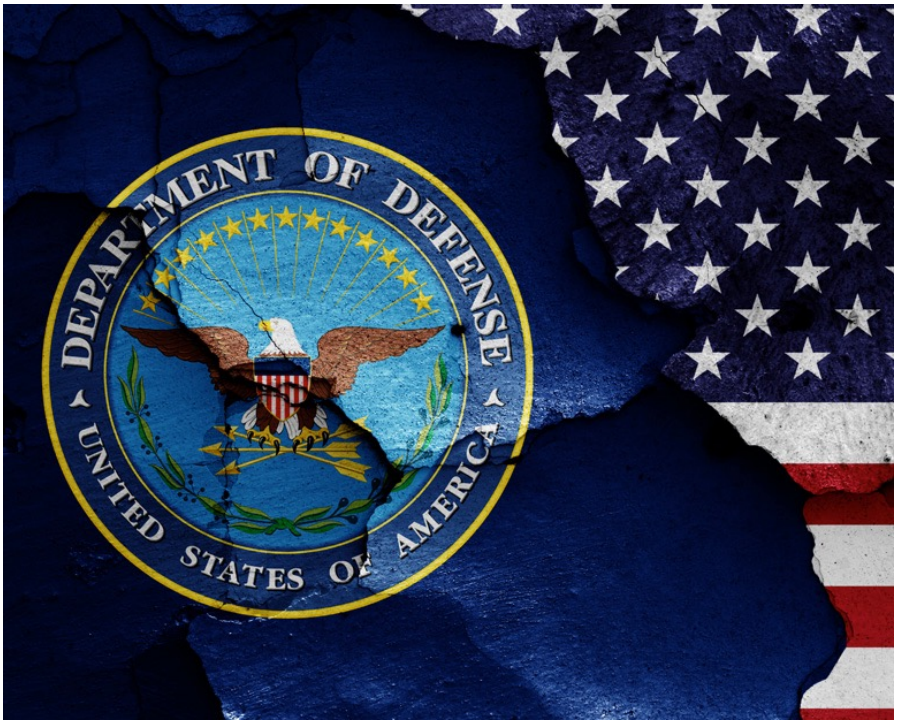
snaptech

CMMC Compliance was officially launched on January 31, 2020.

Every contractor is required to be audited and certified by a third-party auditor (C3PAO) in order to be considered for future contracts.

Required

Yup!



[DoD contractors & subcontractors]

Get **empowered**

The readiness gauge helps you gather insights about your security processes & gaps.

Start preparing for CMMC Compliance Audits today.

Domain: Access Control (AC)

Capability: C001 Establish system access requirements

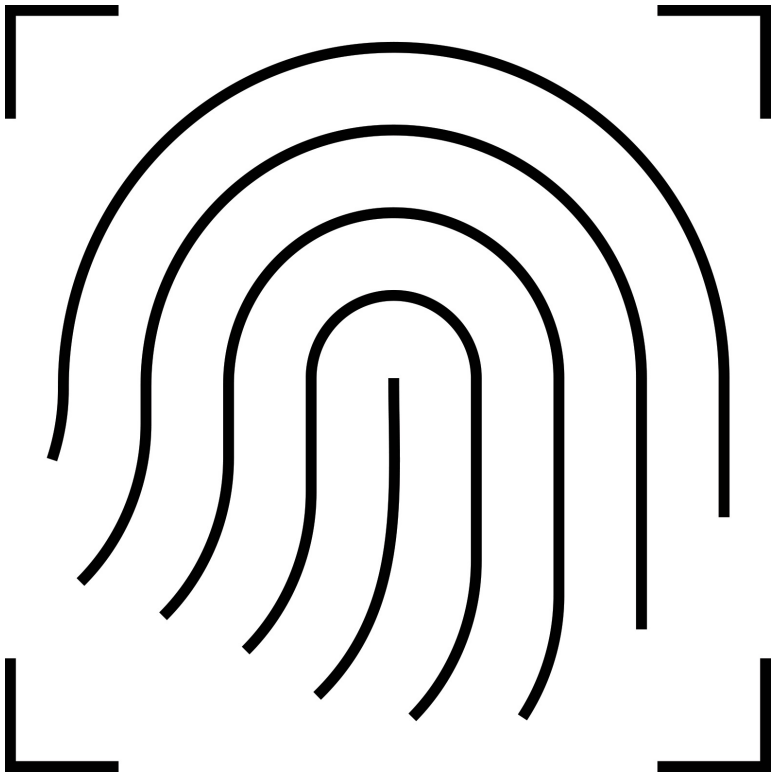
Control: AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems.)

	Yes	No
Do you have a repeatable and auditable process to provision new employee user accounts?	☐	☐
Do you have a repeatable and auditable process to provision new machine accounts on your network?	☐	☐
Do you have a repeatable and auditable process to de-provision employee user accounts?	☐	☐
Do you have a repeatable and auditable process to de-provision machine accounts on your network?	☐	☐
Do you have a standard naming convention for new user accounts and machine accounts?	☐	☐

	Yes	No
Do you understand the specific access requirements for each job role?	☐	☐
Are you using an Identity and Access Management System (IAM), like Active Directory, to manage user and system accounts?	☐	☐
Do you limit user access to only the systems and information they need to complete their assigned work in each line of business application?	☐	☐
Are you reviewing user access on a regular basis?	☐	☐

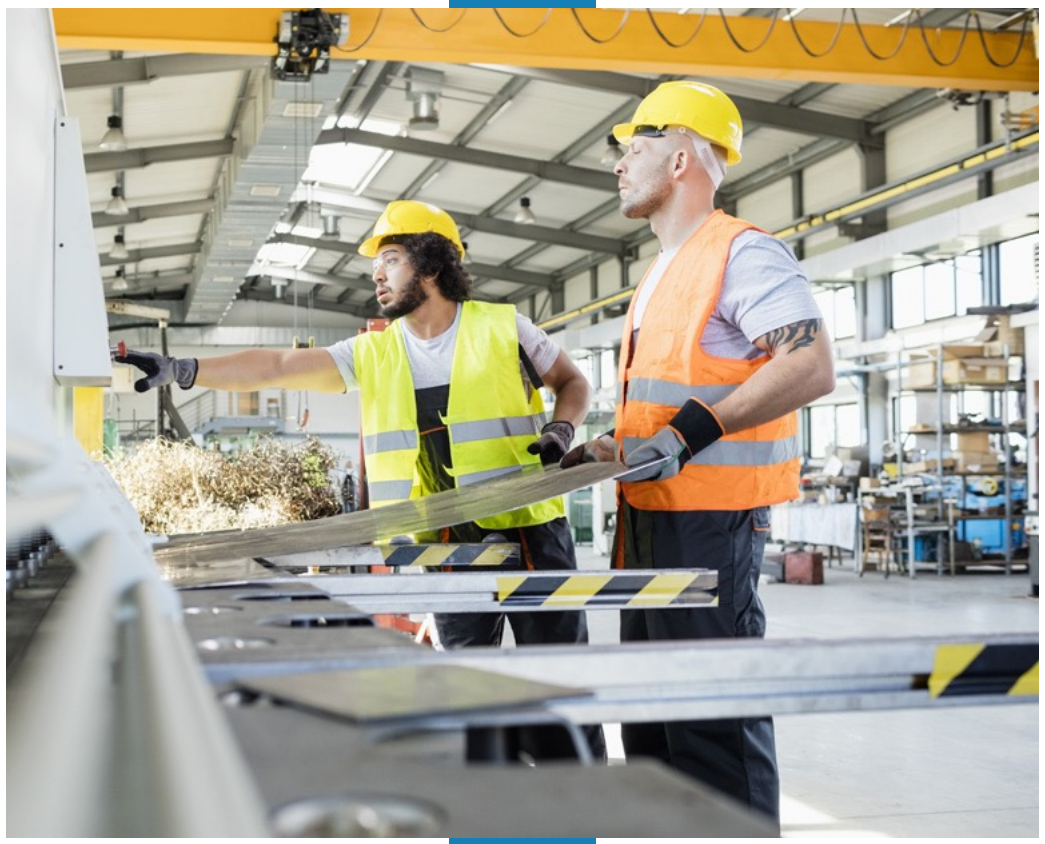
Capability: C002 Control internal system access

Control: AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.



Capability: C004 Limit data access to authorized users and processes

Control: AC.1.003: Verify and control/limit connections to and use of external information systems.



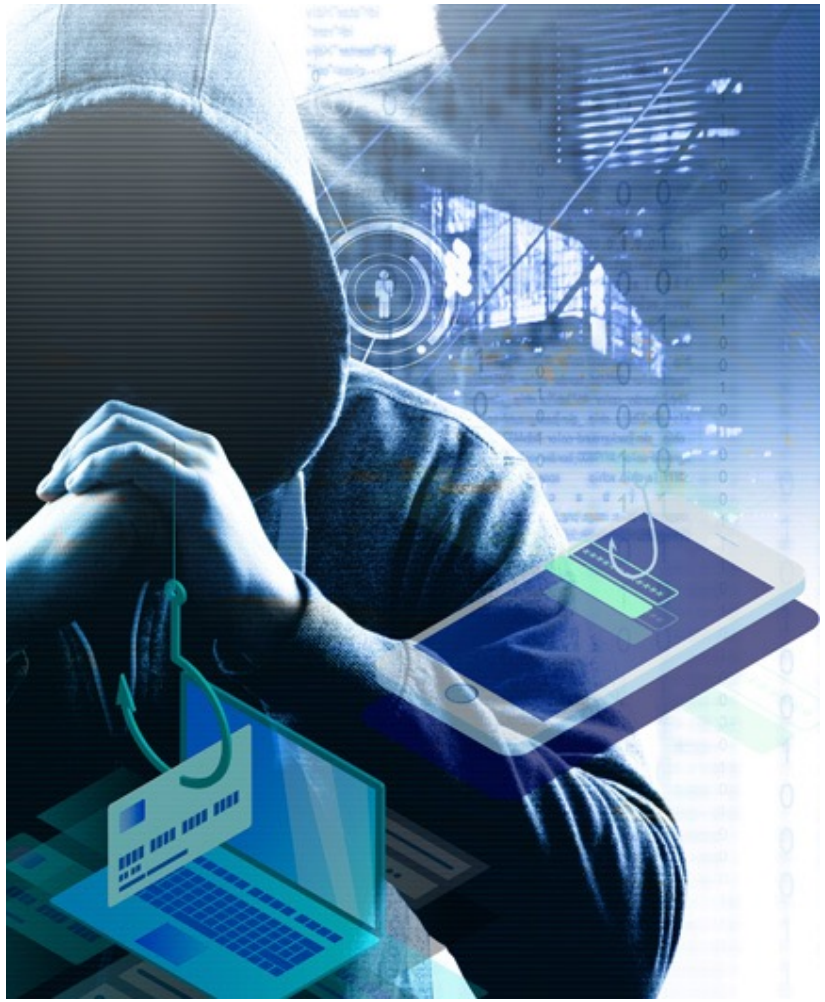
	Yes	No
Do you have an inventory of all the external systems that your company accesses?	☐	☐
Have you documented the nature of the external connections (inbound, outbound, protocol, etc.?)	☐	☐
Do you restrict access to your corporate network to only corporate owned devices?	☐	☐

So... **how are you doing?**

Control: AC.1.004

Control information posted or processed on publicly accessible information systems.

	Yes	No
Do you have a list of users that have access to publish information publicly on your company website, blog, or social media?	☐	☐
Do you have a role in your company to review content for any Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) before it is published publicly?	☐	☐
Do you have a process to review published content to determine if any FCI or CUI information was inadvertently published and remove the content?	☐	☐



Domain: Identification & Authentication (IA)

Capability; C015 Grant access to authenticated entities

Control: IA.1.076: Identify information system users, processes acting on behalf of users or devices.

	Yes	No
Do any of your users share a user ID and password?	☐	☐
Are you able to track and log the user ID for all users and systems that access the company network and applications?	☐	☐

Control: IA.1.076: Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.

	Yes	No
Do you require strong and complex passwords for all your systems and applications?	☐	☐

Domain: Media Protection (MP)

Capability; C024 Sanitize media
Control: MP.1.118 Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.

	Yes	No
Does your company destroy or sanitize all “media” so that it can not be recovered? This includes a wide array of items that can store information, like hard drives, thumb drives, CDs, DVDs, tape backups, etc.	☐	☐
Can you prove that you have destroyed or sanitized all “media,” including printed documents that contain FCI/CUI?	☐	☐

Domain: Physical Protection (PE)

Capability: C028 Limit physical access

Control: PE.1.131: Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.

	Yes	No
Do you maintain a list of personnel with authorized access, and do you issue authorization credentials?	☐	☐
Do you designate areas in your building as “sensitive” and have you put physical security protections in place to limit physical access to the area to only authorized employees?	☐	☐
Are output devices, like printers, placed in areas where their use does not expose data to unauthorized individuals?	☐	☐

Control: PE.1.132: Escort visitors and monitor visitor activity.

	Yes	No
Are personnel required to accompany visitors to areas in a facility with physical access to organization systems?	☐	☐
Do you designate areas in your building as “sensitive” and have you put physical security protections in place to limit physical access to the area to only authorized employees?	☐	☐
Are output devices, like printers, placed in areas where their use does not expose data to unauthorized individuals?	☐	☐

Still **good?**

Control: PE.1.133

Maintain audit logs of physical access.

	Yes	No
Do you require all visitors to sign-in, either electronic or paper, and maintain these records for as long as required?	☐	☐

Control: PE.1.134

Control and manage physical access devices.

	Yes	No
Do you maintain an inventory of all physical access devices, like keys, badges, and key cards?	☐	☐
Is access to your physical access devices limited to only authorized individuals?	☐	☐
Do you manage your physical access \devices? For example, revoking key card access or changing locks as needed.	☐	☐

Domain: System and Communications Protection (SC)

Capability: C039 Control communications at system boundaries

Control: SC.1.175: Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal

	Yes	No
Does your company use firewalls at the external system boundaries to protect systems that handle regulated data?	☐	☐
Does your company use internal firewalls, routers, or switches to segment your internal network?	☐	☐
Do you monitor data flowing in and out of external and internal system boundaries?	☐	☐
Does your company protect data flowing in and out of your external and internal systems by using encryption or tunneling traffic?	☐	☐

This is way too important to not get right the first time.

Schedule a CMMC Consultation

Control: SC.1.176: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

	Yes	No
Does your company have any publicly accessible systems (e.g., internet-facing web servers, VPN gateways, publicly accessible cloud services?)	☐	☐
If so, are these publicly accessible systems physically or logically separated subnetworks (e.g., isolated subnetworks, or Demilitarized Zones DMZ?)	☐	☐

Domain: System & Information Integrity (SI)

Capability: C040 Identify and manage information system flaws

Control: SI.1.210: Identify, report and correct information and information system flaws in a timely manner.

	Yes	No
Does your company have a defined and documented timeframe which system flaws must be identified from vulnerability scans, configuration scans, or manual reviews?	☐	☐
Can you prove that system flaws are identified in accordance with the specified timeframe?	☐	☐
Does your company have a defined and documented timeframe which system flaws must be corrected?	☐	☐
Can you prove that system flaws are corrected in accordance with the specified timeframe?	☐	☐

Control: SI.1.211: Provide protection from malicious code at appropriate locations within organizational information systems.

	Yes	No
Are system components (e.g., workstations, servers, mobile devices) where malicious code protection must be provided identified and documented?	☐	☐

Control: SI.1.212: Update malicious code protection mechanisms when new releases are available.

	Yes	No
Is there a defined frequency by which malicious code protection must be updated?	☐	☐
Does your company actively monitor and update your malicious code protection?	☐	☐

Control: SI.1.213: Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.

	Yes	No
Does your company have a defined and documented frequency for malicious code scans?	☐	☐
Does your company perform real-time malicious code scans on files from external sources as files are downloaded, opened, or executed?	☐	☐

How **did you do?**

If you answered "No" to more than 3 or 4 of these questions, your organization has a lot to do in order to become CMMC Compliant.

Don't worry, we can help get you ready.

Let's book some time together to create a step-by-step readiness plan and keep you on track.

Schedule a CMMC Consultation