Microsoft

Microsoft CMMC 2.0

Level 1 Implementation Guide

Written By SUMMIT7

Purpose 3
What Is CMMC? 3
Who Needs CMMC? 4
What Determines My CMMC Level Requirement? 4
What is Maturity Level 1? 5
Microsoft 365 Licensing for Maturity Level 1 5
Microsoft 365 Implementation for CMMC Maturity Level 1 6
Access Control (AC) 7
AC. L1-3.1.1 - Authorized Access Control 7
AC. L1-3.1.2 - Transaction and Function Control 9
AC. L1-3.1.20- External Connections 11
AC. L1-3.1.22 - Control Public Information 13
Identification and Authentication (IA) 14
IA. L1-3.5.1 - Identification 15
IA. L1-3.5.2 - Authentication 16
Media Protection (MP) 18
MP. L1-3.8.3 - Media Disposal 18
Physical Protection (PE) 20
PE. L1-3.10.1 - Limit Physical Access 20
PE. L1-3.10.3 - Escort Visitors 22
PE. L1-3.10.4 - Physical Access Logs 23
PE. L1-3.10.5 - Manage Physical Access 24
System and Communications Protection (SC) 25
SC. L1-3.13.1 - Boundary Protection 26
SC. L1-3.13.5- Public-Access System Separation 28
System and Information Integrity (SI) 29
SI. L1-3.14.1 - Flaw Remediation 30
SI. L1-3.14.2 - Malicious Code Protection 32
SI. L1-3.14.4 - Update Malicious Code Protection 33
SI. L1-3.14.5 - System & File Scanning 35

Purpose

This guide is intended to provide small and medium-sized organizations with guidance for using Microsoft 365 (M365) to satisfy the Cybersecurity Maturity Model Certification (CMMC) Level 1 requirements.

What Is CMMC?

CMMC is a standard designed for the implementation of cybersecurity across the United States Defense Industrial Base (DIB) to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The DIB is made up of over 300,000 commercial organizations that produce or provide products and services to the United States Department of Defense (DoD) as a part of the execution of a contract.

The CMMC program is intended to validate the ability of DIB organizations to adequately protect sensitive unclassified information. The capabilities of organizations are validated against the CMMC security control framework and companies are awarded a certification from 1 of the 3 possible maturity levels (ML1, ML2, and ML3). Each maturity level is assigned a specified set of security and privacy controls that the organization must satisfy to achieve the associated level.

Each maturity level of the CMMC standard is constructed using a determined set of security controls from the CMMC framework. The CMMC framework is currently comprised of the administrative and technical requirements found within the 110 security controls of National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171). These controls are divided amongst the following 14 control families:

Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Who Needs CMMC?

The Defense Federal Acquisition Regulation Supplement (DFARS) contract clause 252.204-7021 will begin to be included as a condition of contract award for Department of Defense (DoD) contracts as soon as Spring 2023; this clause will eventually be present in all contracts issued by the DoD.

This contract clause will allow the issuing agency to require a DIB contractor to possess and maintain the CMMC maturity level designated within the clause. The certification level requirement is dictated by the importance and sensitivity of the data supplied or created as a part of the contract's intended fulfillment.

Each maturity level of the CMMC standard is constructed using a determined set of security controls from the CMMC framework. The CMMC framework currently is comprised of the administrative and technical requirements.

What Determines My CMMC Level Requirement?

The contents of an organization's prime contracting or sub-contracting agreement will contain the DFARS 252.204-7021 contract clause. This contract clause will dictate the minimum CMMC maturity level an organization must have achieved prior to being awarded the contract.

DoD contracts which only transfer and/or create FCI will require organizations to achieve a CMMC Maturity Level 1 certification to self-attest to compliance with the 17 specified security controls from the CMMC framework. Organizations must satisfy the requirements to achieve this maturity level.

DoD contracts that transfer and/or create CUI, or include DFARS clause 252.204-7012, may require organizations to satisfy all 110 security controls of the CMMC framework to obtain a CMMC Maturity Level 2 certification. This maturity level requires organizations to undergo an assessment from a CMMC 3rd Party Assessment Organization (C3PAO) to validate their compliance with the applicable security controls.

As of this publication, the requirements to obtain CMMC Maturity Level 3 have not been finalized. As CMMC is an additive framework in nature, organizations can expect to satisfy all 110 security requirements found in Maturity Levels 1 and 2. Additionally,

organizations will have to satisfy additional security controls which will be extracted from the National Institutes of Standards and Technology (NIST) Special Publication 800-172.

What Is Maturity Level 1?

CMMC Maturity Level 1 (ML1) is the lowest of the CMMC certification levels. Its requirements consist of basic cybersecurity practices of 17 security controls extracted from the following six CMMC security families:

Access Control	Identification And Authentication	Media Protection
Physical Protection	Systems and Communication Protection	System and Information Integrity

These security controls are also the Basic Safeguarding requirements imposed on covered contractor information systems as a part of Federal Acquisitions Regulation (FAR) 52.204-21.

Microsoft 365 Licensing for Maturity Level 1

To satisfy the requirements found in CMMC Maturity Level 1, organizations must implement basic cyber hygiene principles throughout the information system which will be used to store, process, or transmit FCI in performance of their DoD contract. Among the requirements, the organization will need to establish strong access control, identification, and authentication capabilities for all users and devices. Additionally, Maturity Level 1 requires organizations to become proactive with resolving system flaws, protect from malicious threats, and increase their awareness of the connections to and from their information system.

Based on the requirements of the 17 controls applicable to CMMC Maturity Level 1, an organization in need of satisfying these requirements should leverage the products and features associated with Microsoft 365 E3 licensing. The M365 E3 license empowers

organizations with the capabilities of Azure Active Directory (Azure AD), Microsoft Intune, and Microsoft Defender for Endpoint; these features can be leveraged by organizations as solutions independently or complementary to one another to satisfy the requirements of CMMC Maturity Level 1.

To assure proper due diligence is taken before securing Microsoft licensing, the organization must not only fully evaluate current contractual requirements and sensitivity levels of the data that they handle, but also determine whether future business strategies may include contracts with higher CMMC maturity level requirements.

The implementation guidance provided within this document is designed to help organizations meet the minimum data safeguarding requirements attached to FCI. Although the products and services recommended by this guide do not fully represent the features required to meet the higher maturity levels of CMMC. The increased safeguarding requirements of the remaining higher maturity levels of CMMC would require additional M365 products and their applicable licenses.

Microsoft 365 Implementation for CMMC Maturity Level 1

This section will provide the organization with guidance to configure the products and services acquired with their M365 E3 licensing to satisfy the technical requirements of CMMC Maturity Level 1. However, the organization will still be responsible for developing procedures to carry out the actionable tasks found within the requirements.

The CMMC Maturity Level 1 certification is comprised of 17 security controls of the CMMC framework. Each control contains a control statement or the **control language.** This statement describes what the control is intended to accomplish (sometimes referred to as the "outcome" of the control). To achieve the outcome described by the **control language,** each control contains a series of **determination statements** which are individual tasks that must be satisfied for a control to be considered implemented.

Implementing CMMC Maturity Level 1 with M365 E3 licensing will also place organizations in a better position to graduate their CMMC maturity level if necessary. The products and services found in the M365 E3 license serve as the foundations for the licensing required to meet the more advanced level(s) of the standard.

Access Control (AC)

To satisfy the CMMC Maturity Level 1 requirements of the Access Control (AC) control family; the following products of the Microsoft 365 E3 license will be used (each hyperlink will direct you to an overview of the product):

Control	M365 Product
AC. L1- 3.1.1 - Authorized Access Control	▫ Azure Active Directory (Azure AD) ▫ Conditional Access ▫ Azure Role-Based Access Control (Azure RBAC) ▫ Microsoft Intune
AC. L1-3.1.2 - Transaction and Function Control	▫ Azure Active Directory (Azure AD) ▫ Azure Role-Based Access Control (Azure RBAC)
AC. L1-3.1.20- External Connections	▫ Azure Active Directory (Azure AD) ▫ Conditional Access ▫ Microsoft Defender for Endpoint – Microsoft Defender for Endpoint Plan 1 ▫ Microsoft Defender Antivirus ▫ Windows Defender Firewall ▫ Microsoft Intune
AC. L1-3.1.22 - Control Public Information	▫ Azure Active Directory (Azure AD) ▫ Azure Role-Based Access Control (Azure RBAC)

AC. L1-3.1.1 - Authorized Access Control

Control language:

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

Determination statements:

[a] authorized users are identified

[b] processes acting on behalf of authorized users are identified

[c] devices (and other systems) authorized to connect to the system are identified

[d] system access is limited to authorized users

[e] system access is limited to processes acting on behalf of authorized users

[f] system access is limited to authorized devices (including other systems)

Control summary:
The organization must develop a process to identify what people, processes, and technologies are authorized to access organization-controlled resources.

Once authorized users and devices are identified, security controls must be put in place to limit their access to only the resources to which they are authorized.

Microsoft 365 licensing required:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD)- Azure AD Premium Plan 1, Conditional Access
- Azure Role-Based Access Control (Azure RBAC)
- Microsoft Intune

How to implement using Microsoft 365:

To successfully meet this requirement an organization will need to maintain an active roster of all assets (people, processes, and technologies) authorized for access to organizational resources *[a,b,c]*.

Additionally, the organization will need to limit access to only authorized assets by using **Azure AD** and **Microsoft Intune**.

Authorized users will need to have accounts created in **Azure AD** with Username, Password, and Multifactor Authentication access controls in place. Furthermore, it is best practice to classify all users in **Azure AD** based on roles using **Azure AD Role-Based**

Access Control (Azure AD RBAC). Non-Privileged user accounts should be assigned to a role with read-only permissions for Microsoft 365 resources.

Authorized devices (Windows 10/11, macOS, iOS, Android) would need to be enrolled using **Microsoft Intune** to gain access to Microsoft 365 resources.

Azure AD combined with **Microsoft Intune** allows the organization to create conditional access policies (policies that allow you to control access for users and devices). Additionally, system access for user accounts and devices can be controlled by creating security groupings and assigning members (users, devices) to the group, and assigning group access to authorized resources. This process will dictate their ability to access content stored within Microsoft 365 (i.e., Exchange, SharePoint, OneDrive, Microsoft Teams) *[d,e,f]*.

Microsoft technical reference documentation:

Enrolling Windows 10/11 devices in Intune

Enrolling macOS devices in Intune

Enrolling iOS devices in Intune

Enrolling Android devices in Intune

What is Azure Role-Based Access Control?

Assigning user roles in Azure

Creating groups in Azure AD

Implementing conditional access with Azure

Grant user access to resources using Azure

AC. L1-3.1.2 - Transaction and Function Control

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

Determination statements:

[a] the types of transactions and functions that authorized users are permitted to execute are defined

[b] system access is limited to the defined types of transactions and functions for authorized users

Control summary:
The organization must document the different user roles and capabilities those roles are allowed to perform when using organizational resources.

The organization will need to place technical restrictions on user accounts to prevent them from performing unauthorized actions.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD) - Azure Active Directory Premium Plan 1
- Azure Role-Based Access Control (Azure RBAC)

How to implement using Microsoft 365:

To successfully implement this control, the organization will need to create a document which lists all types of user roles which will be deployed on the information system. This document must also list the types of actions each specified role is permitted to perform *[a]*.

Using **Azure AD** and **Azure RBAC,** the organization can classify users based on their documented roles. **Azure RBAC** allows for the fine-tuning of user role permissions to enable the organization to restrict what resources the user can access and what they are allowed to do when they are accessing them. These permissions will need to align with capabilities defined within organizational documentation *[b]*.

Microsoft technical reference documentation:

What is Azure role-based access control (Azure RBAC)? | Microsoft Docs

Assigning user roles in Azure

AC. L1-3.1.20- External Connections

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

Determination statements:

[a] connections to external systems are identified

[b] the use of external systems is identified

[c] connections to external systems are verified

[d] the use of external systems is verified

[e] connections to external systems are controlled/limited

[f] the use of external systems is controlled/limited

Control summary:

The organization will need to control and manage connections between both internal and external resources, connections to cloud services, and network connectivity devices (routers, wireless access points). This includes:

i. Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information
ii. Limiting connections to outside systems from the internal network
iii. Limiting connections from external systems to internal resources

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD) - Azure Active Directory Premium Plan 1, Conditional Access
- Microsoft Defender for Endpoint – Microsoft Defender for Endpoint Plan 1, Microsoft Defender Antivirus Windows Defender Firewall
- Microsoft Intune

How to implement using Microsoft 365:

The organization will need to create documentation designed to outline the information and data flow on the network, as well as network diagrams that call out the external connections (VPN, Cloud applications, etc.) *[a,b]*.

Microsoft Defender for Endpoint includes an endpoint firewall, **Windows Defender Firewall**, which will need to be enabled on the endpoint connecting to the information system using **Microsoft Intune. Microsoft Defender for Endpoint** offers **Network protection** capabilities which helps prevent access to dangerous web domains via applications. Domains that host phishing scams, exploits, and other malicious content on the Internet are considered dangerous. Network protection must be configured to block all outbound HTTP(s) traffic that attempts to connect to low-reputation sources (based on the domain or hostname) *[c,d]*.

Using **Azure AD** and **Microsoft Intune,** the organization will enable conditional access policies for users and devices. These policies will include limiting user access to company resources based on roles, device type, and/or location. Users can be limited to connecting to company resources by only using company-approved, owned, or registered devices. The organization may also choose to add geographical restrictions to user logins through conditional access. This requires assets attempting to connect to the system to be identified and verified prior to being granted access to the system *[c,d,e,f]*.

Microsoft technical reference documentation:

Best Practices for configuring Windows Defender Firewall

Enabling Windows Defender Firewall

Implementing conditional access with Azure

Overview of Network Protection

AC. L1-3.1.22 - Control Public Information

Control language:
Control information posted or processed on publicly accessible information systems.

Determination statements:

[a] individuals authorized to post or process information on publicly accessible systems are identified

[b] procedures to ensure FCI is not posted or processed on publicly accessible systems are identified

[c] a review process is in place prior to posting any content to publicly accessible systems

[d] content on publicly accessible systems is reviewed to ensure that it does not include FCI

[e] mechanisms are in place to remove and address improper posting of FCI

Control summary:

The organization is responsible for preventing FCI data from being publicly posted without permission. The organization must control who possesses the capabilities to not only access FCI on the information system, but also identify who is authorized to distribute information to the public. To ensure that FCI does not get distributed without permission, is removed, or incorrectly/accidentally distributed, the organization must develop a process to review and authorize information prior to distribution. Additionally, the organization will need a process in place to remove or retract information incorrectly shared.

Microsoft 365 licensing needed:
Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD)- Azure Active Directory (Azure AD) - Azure Active Directory Premium Plan 1
- Azure Role-Based Access Control (Azure RBAC)

How to implement using Microsoft 365:

Using a combination of documented policies and procedures in addition to enforcement of access permissions through **Azure AD and Azure RBAC,** the organization will need to authorize personnel who are permitted to distribute information to the public on behalf of the company *[a,b].* For a user to post FCI, the user must have access to the information system and file directory where the data is stored. For this to happen, they would have to be granted access by role using **Azure AD**.

To assure that FCI is not publicly posted intentionally or unintentionally, the organization will need to develop a process for the review of all content prior to public release. This review process should include a review of the content to ensure it does not include FCI prior to authorization being granted for distribution *[c,d].*

Finally, the organization must have a documented process for the removal of FCI accidentally posted to public forums without authorization. This process must include the removal of the data, potential consequences for the responsible party, and an after-action review to identify ways to prevent similar instances in the future *[e].*

Microsoft technical reference documentation:

Grant a user access to resources using Azure

Identification and Authentication (IA)

To satisfy the CMMC Maturity Level 1 requirements of the Identification and Authentication (IA) control family; the following products of the Microsoft 365 E3 license will be used (each hyperlink will direct you to an overview of the product):

Control	M365 Product
IA. L1-3.5.1 - Identification	▫ Azure Active Directory (Azure AD) ▫ Azure AD Multifactor Authentication ▫ Conditional Access ▫ Microsoft Intune
IA. L1-3.5.2 - Authentication	▫ Azure Active Directory (Azure AD) ▫ Azure AD Multifactor Authentication ▫ Microsoft Intune

IA. L1-3.5.1 - Identification

Control language:

Identify information system users, processes acting on behalf of users, or devices.

Determination statements:

[a] system users are identified

[b] processes acting on behalf of users are identified

[c] devices accessing the system are identified

Control summary:

This control requires an organization to assign unique identifiers to users and devices authorized to access organizational assets. It also requires an automated process to be assigned to user IDs associated with the responsibility of the tasks the process is designed to perform. This is used to establish undeniable identification of the user, device, or process while it performs actions on organizational assets.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD)- Azure Active Directory Premium Plan 1
- Microsoft Intune

How to implement using Microsoft 365:

The organization will establish and document a universal standard for user and device identifiers on the information system. This document will provide guidance for the creation of user accounts allowing them to be associated with a particular user and their actions. When the user account is created in **Azure AD,** the organization will create the user account using the established standard *[a]*.

Any automated processes or scripts which act on behalf of users should be assigned to the user **Azure AD** which they are being performed in accordance with *[b]*.

Devices authorized for access to resources will need to be enrolled in **Microsoft Intune** and assigned unique device ids in **Azure AD** *[c]*.

Microsoft technical reference documentation:

Adding Users in Azure AD

Enrolling devices in Microsoft Intune

IA. L1-3.5.2 - Authentication

Control language:

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

Determination statements:

[a] the identity of each user is authenticated or verified as a prerequisite to system access

[b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access

[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access

Control summary:
The organization will need to implement access control mechanisms which require any identity (user, device, process) attempting to access organizational resources to authenticate and verify their identity prior to access being granted to resources.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD)- Azure AD Premium Plan 1, Azure AD Multifactor Authentication, Conditional Access
- Microsoft Intune

How to implement using Microsoft 365:

To satisfy this requirement the organization will need to use conditional access within **Azure AD** to create conditional access policies that require Azure MFA for all authorized user accounts as a prerequisite to access the information system *[a]*.

Using **Microsoft Intune** to enroll devices and **Azure AD** to configure conditional access policies for user accounts, the organization can require that user accounts only connect to the information system with devices enrolled in **Microsoft Intune** *[c]*. At user sign-on, **Azure AD** will deny access to the user if the device being used to connect is not one enrolled with **Microsoft Intune.**

To comply with requirements AC.L1-3.1.1 and IA.L1 3.5.1 the organization would have to identify authorized processes executed by users. Processing acting on behalf of users (if present), which are assigned to user accounts, will require the attached user to identify and authenticate prior to access to the system *[b,c].*

Microsoft technical reference documentation:

Implementing conditional access with Azure

Enrolling devices in Microsoft Intune

Configuring Azure AD Multi-Factor Authentication

Media Protection (MP)

Organizations are not required to leverage solutions found in the Microsoft 365 E3 license to satisfy the CMMC Maturity Level 1 requirements of the Media Protection (MP) control family. Instead, organizations can implement documented policies & procedures and carry out process tasks to satisfy the requirements.

MP. L1-3.8.3 - Media Disposal

Control language:

Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.

Determination statements:

[a] system media containing FCI is sanitized or destroyed before disposal

[b] system media containing FCI is sanitized before it is released for reuse

Control summary:

This requirement applies to all media, both digital and traditional, subject to disposal or reuse. The organization maintains a responsibility to limit the spillage and unauthorized access of data by either destroying system components used to store FCI prior to disposing of or reusing the assets. Examples include, but are not limited to, digital storage components found in devices, portable storage devices, or mobile devices. The intent of this process is to prevent the retrieval or reconstruction of sensitive information from the device.

NIST SP 800-88 provides guidance on best practices for media sanitation.

Microsoft 365 licensing needed:

- Solutions found in the Microsoft 365 E3 license are not required to satisfy this requirement. Organizations should implement documented policies & procedures and carry out process tasks to satisfy this requirement.

How to implement:

NIST SP 800-88 documentation lists clear, purge, and destroy as acceptable media sanitation techniques as:

- ***Clear*** *- applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).*
- ***Purge*** *- applies physical or logical techniques that render Target Data recovery infeasible using state-of-the-art laboratory techniques.*
- ***Destroy -*** *renders Target Data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data -* *NIST SP 800-88.*

For purposes of satisfying this control, the organization should create a media sanitation procedural document which requires that all system media be either **cleared, purged, or destroyed** prior to reuse or disposal. Devices intended for re-use, such as endpoints and mobile devices, should be wiped clean of all data and reset to factory defaults prior to the re-issuance of the devices *[a,b]*.

Devices intended for disposal should be restored to factory settings, wiped clean of all previous store data, and destroyed using methods that disintegrate, pulverize, melt, or incinerate the device prior to disposal *[a].*

Microsoft technical reference documentation:

None

Physical Protection (PE)

For this guide, the assumption is that the organization is utilizing a full suite of Microsoft cloud services. The Microsoft implementation of FedRAMP requirements help ensure Microsoft in-scope cloud services meet or exceed the requirements of CMMC. This allows organizations to assume that in execution of their contract with Microsoft, physical protections must be adequate to satisfy CMMC requirements.

The organization will still assume responsibilities to successfully implement the control to prevent unauthorized disclosure of information accessed or discussed. Physical protections will need to be in place to prevent FCI from being seen while also being accessed in organizationally controlled spaces. An organization may also interact with physical forms of FCI in the performance of a contract for each physical control, and the organization will assume all responsibility to successfully implement the measures to prevent unauthorized disclosure of information stored.

PE. L1-3.10.1 - Limit Physical Access

Control language:

Limit physical access to organization information systems, equipment, and the respective operating environments to authorized individuals.

Determination statements:

[a] authorized individuals allowed physical access are identified

[b] physical access to organizational systems is limited to authorized individuals

[c] physical access to equipment is limited to authorized individuals

[d] physical access to operating environments is limited to authorized individuals

Control summary:

This control requires organizations to create physical protections to prevent unauthorized access to physical or logical data storage locations. The organization must identify who has access to both physical and logical data and place physical measures in place to stop those not authorized to access resources.

Microsoft 365 licensing needed:

- Solutions found in the Microsoft 365 E3 license are not required to satisfy this requirement. Organizations should implement documented policies & procedures and carry out process tasks to satisfy this requirement.

How to implement:

The organization will need to create a list which details all personnel authorized to access organizationally owned spaces *[a]*; this includes granular details of specially protected areas of the physical environment where greater restrictions for access are put into place.

The organization will need to demonstrate that physical boundaries are put in place to prevent unauthorized access to organizational owned devices and areas. This can be accomplished through constructing fences, locking doors and windows, etc. *[b,c,d]*

Microsoft technical reference documentation:

None

PE. L1-3.10.3 - Escort Visitors

Control language:

Escort visitors and monitor visitor activity

Determination statements:

[a] visitors are escorted

[b] visitor activity is monitored

Control summary:

The organization is responsible for restricting access to their physical environment to only authorized personnel. Any person without a normal DTD business need to access the organization's facilities must be escorted and always monitored while on site.

Microsoft 365 licensing needed:

- Solutions found in the Microsoft 365 E3 license are not required to satisfy this requirement. Organizations should implement documented policies & procedures and carry out process tasks to satisfy this requirement.

How to implement:

The organization must document all personnel with an authorized business need to access their physical facilities. Organizational policies and procedures must indicate, and the organization must execute the following for all personnel not listed on the organizations authorized access roster:

1. The visitor must sign in and out of a visitor log when arriving and departing the facility *[a,b]*
2. The visitor must wear a badge or other identifier to establish that they are a visitor to the facility *[b]*
3. The visitor must always be escorted while on company property protected by physical access controls*[b].*

Microsoft technical reference documentation:

None

PE. L1-3.10.4 - Physical Access Logs

Control language:

Maintain audit logs of physical access devices

Assessment objective:

[a] audit logs of physical access are maintained

Control summary:

An audit log of physical access can either be a physical document detailing personnel who have accessed areas of the facility or automated logging of physical access devices such as badge readers. This includes areas of initial facility access, restricted access for areas of sensitive assets, or a combination of the two. No matter the method of access control logging (physical or automated) the organization will need to maintain a record of the entries into the log.

Microsoft 365 licensing needed:

- Solutions found in the Microsoft 365 E3 license are not required to satisfy this requirement. Organizations should implement documented policies & procedures and carry out process tasks to satisfy this requirement.

How to implement:

The organization will need to determine the method for restricting access to areas not designated for the public. In areas where facility access must be restricted for any reason, the organization is required to maintain logs of access events for these designated areas. This can be achieved by maintaining a physical sign-in sheet-type

document where physical access to the areas can be recorded. In the case of digital badge readers or other electronic physical access devices with built-in logging capabilities; the organization must develop a process to retain the digital logs created for a determined period *[a].*

Microsoft technical reference documentation:

None

PE. L1-3.10.5 - Manage Physical Access

Control language:

Control and manage physical access devices

Determination statements:

[a] physical access devices are identified

[b] physical access devices are controlled

[c] physical access devices are managed

Control summary:

This control requires organizations to identify the devices which will be used to restrict access to areas of the facility which require additional protective measures. The organization will also need to maintain control of the devices used to restrict access to identified areas as well as manage who has access capabilities to bypass the access controls the devices are intended to provide.

This could include limiting the replication of physical keys to a list of authorized personnel or controlling who has management capabilities for logical access control devices such as badge readers.

Microsoft 365 licensing needed:

- Solutions found in the Microsoft 365 E3 license are not required to satisfy this requirement. Organizations should implement documented policies & procedures and carry out process tasks to satisfy this requirement.

How to implement:

In the organization's asset inventory, assets used to provide physical protection should be identified and documented. Badge readers, Locks, cameras, and other physical access control devices should all be accounted for and documented *[a]*. The organization will need to identify through documented policies and procedures how they intend to control maintenance and configuration of the identified physical control devices and who is authorized to perform these tasks *[b].* This can include tasks such as controlling who can make keys to physical locks, adding users, or issuing access mechanisms such as keys, keycards, access pin numbers, etc. This should also include the creation of an authorization process to approve changes to the devices and the issuing of the access control mechanisms to personnel *[c].*

Microsoft technical reference documentation:

None

System and Communications Protection (SC)

To satisfy the CMMC Maturity level 1 requirements of the System and Communication Protection (SC) control family; the following products of the Microsoft 365 E3 license will be used (each hyperlink will direct you to an overview of the product):

Control	M365 Product
SC. L1-3.13.1 - Boundary Protection	▫ Azure Active Directory (Azure AD) ▫ Conditional Access ▫ Microsoft Defender for Endpoint – Microsoft Defender for Endpoint Plan 1 ▫ Microsoft Defender Antivirus ▫ Windows Defender Firewall ▫ Network Protection ▫ Microsoft Intune
SC. L1-3.13.5- Public-Access System Separation	▫ Azure Active Directory (Azure AD) ▫ Azure AD Multifactor Authentication ▫ Conditional Access ▫ Microsoft Intune

SC. L1-3.13.1 - Boundary Protection

Control language:

Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems

Determination statements:

[a] the external system boundary is defined

[b] key internal system boundaries are defined

[c] communications are monitored at the external system boundary

[d] communications are monitored at key internal boundaries

[e] communications are controlled at the external system boundary

[f] communications are controlled at key internal boundaries

[g] communications are protected at the external system boundary

[h] communications are protected at key internal boundaries.

Control summary:

The organization will need to detail system boundaries by identifying areas of entry and exit which exist on the information system. Once identified the organization will need to put access control measures and network traffic mechanisms in place to limit the internal connections to external resources as well as the external connections made to their resources.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD) - Azure AD Premium Plan 1, Conditional Access
- Microsoft Defender for Endpoint- Microsoft Defender for Endpoint Plan 1, Microsoft Windows Defender Firewall, Microsoft Defender Antivirus, Network Protection
- Microsoft Intune

How to implement using Microsoft 365:

The organization will need to create documentation designed to outline the information and data flow on the network, as well as network diagrams that call out the external and key internal boundaries for assets access (e.g. cloud applications, endpoints, etc.) *[a,b]*.

Microsoft Defender for Endpoint includes an endpoint firewall, **Windows Defender Firewall**, which will need to be enabled on the endpoint connecting to the information system using **Microsoft Intune. Microsoft Defender for Endpoint** offers **Network protection** capabilities which helps prevent access to dangerous web domains and application. Domains that host phishing scams, exploits, and other malicious content on the Internet are considered dangerous. Network protection must be configured to block all outbound HTTP(s) traffic that attempts to connect to low-reputation sources (based on the domain or hostname) *[c,d,g,h].*

Using **Azure AD and Microsoft Intune,** the organization can create conditional access policies which make sure only authorized users and managed & compliant devices can

access Microsoft 365 services such as email and Software as a service (SaaS) applications *[e,f]*.

Microsoft technical reference documentation:

Best Practices for configuring Windows Defender Firewall

Enabling Windows Defender Firewall

Implementing conditional access with Azure

Overview of Network Protection

SC. L1-3.13.5- Public-Access System Separation

Control language:

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

Determination statements:

[a] publicly accessible system components are identified

[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks

Control summary:

For all organization resources which can be accessed by the public, there must be physical and/or logical separation created from network resources which house FCI. Logical separation can be enforced with boundary control mechanisms and techniques such as firewalls, routers, and gateways for on-premises infrastructure. Cloud based surfaces with identification and authentication mechanisms in place also create logical boundaries for the FCI which is stored within.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Azure Active Directory (Azure AD) - Azure AD Premium Plan 1, Conditional Access, Azure Multi-Factor Authentication (MFA)
- Microsoft Intune

How to implement using Microsoft 365:

The organization will need to maintain a list of all controlled systems able to be accessed publicly and assure that those components are not attached to the same Microsoft 365 environment as FCI *[a]*.

Using **Azure AD** and **Microsoft Intune,** the organization will need to set conditional access policies which restrict access to the information system to authorized users and devices. This creates a logical password and multifactor authentication protected boundary for access to the FCI environment *[b]*.

Microsoft technical reference documentation:

Configuring Azure AD Multi-Factor Authentication

Implementing conditional access with Azure

System and Information Integrity (SI)

To satisfy the CMMC Maturity Level 1 requirements of the System and Information Integrity (SI) control family; the following products of the Microsoft 365 E3 license will be used (each hyperlink will direct you to an overview of the product):

Control	M365 Product
SI. L1-3.14.1 - Flaw Remediation	▫ Microsoft Intune

SI. L1-3.14.2 - Malicious Code Protection	▫ Microsoft Defender for Endpoint – Microsoft Defender for Endpoint Plan 1 ▫ Microsoft Defender Antivirus ▫ Microsoft Intune ▫ Exchange online protection
SI. L1-3.14.4 - Update Malicious Code Protection	▫ Microsoft Defender for Endpoint – Microsoft Defender for Endpoint Plan 1 ▫ Microsoft Defender Antivirus ▫ Microsoft Intune
SI. L1-3.14.5 - System & File Scanning	▫ Microsoft Defender for Endpoint – Microsoft Defender for Endpoint Plan 1 ▫ Microsoft Defender Antivirus ▫ Microsoft Intune

SI. L1-3.14.1 - Flaw Remediation

Control language:

Identify, report, and correct information and information system flaws in a timely manner.

Determination statements:

[a] the time within which to identify system flaws is specified

[b] system flaws are identified within the specified time frame

[c] the time within which to report system flaws is specified

[d] system flaws are reported within the specified time frame

[e] the time within which to correct system flaws is specified

[f] system flaws are corrected within the specified time frame

Control summary:
A developed process to identify and resolve flaws within the information system must be created. The organization will be responsible for setting a standard that will allow the organization to identify the flaw, analyze its severity, and apply items such as patches or compensating solutions to resolve it.

The organization is also responsible for assuring that the process put in place is executed as specified. Meaning that flaws are resolved in the time frame which they determined was the standard.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Microsoft Intune
- Defender for Endpoint (Plan 1)
- Exchange Online Protection
- Microsoft Defender Antivirus

How to implement using Microsoft 365:

The organization will need to develop policy and procedure documentation that requires and facilitates the organization checking vendor resources such as websites or direct notifications for available patches on a recurring basis. [a].

Additionally, the documentation should develop a process to evaluate the updates for severity and determine a mandatory time frame for the updates to be applied to remove flaws based on their severity *[c,e].*

In accordance with the time periods specified, devices enrolled and controlled using **Microsoft Intune,** should be configured to check for and automatically apply updates to systems *[b,e]*.

Finally, the organization will need to implement a review process for system flaw remediation activities. During this process, remediated flaws will be evaluated to determine if they were resolved within the time period specified in the documented procedures created by the organization. Using **Microsoft Intune,** the organization can

produce on-demand device compliance reports that will provide visibility for items such as patch status of enrolled devices *[f].*

Microsoft technical reference documentation:

Managing Windows updates with Intune

Device Compliance Reports using Intune

SI. L1-3.14.2 - Malicious Code Protection

Control language:

Provide protection from malicious code at appropriate locations within organizational information systems.

Determination statements:

[a] designated locations for malicious code protection are identified

[b] protection from malicious code at designated locations is provided

Control summary:

The organization must maintain an up-to-date inventory of all endpoints that access the information system, and the organization must have malicious code protection mechanisms such as anti-virus/anti-malware solutions deployed to those identified locations.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Microsoft Defender for Endpoint- Microsoft Defender for Endpoint Plan 1, Microsoft Defender Antivirus

- Microsoft Intune
- Exchange Online Protection

How to implement:

To identify the locations for malicious code protection, the organization will need to develop and maintain an inventory of assets which access their resources. Additionally, through a network diagram, the organization will need to identify areas on entry into the information system, which are the avenues that can be used to introduce malicious code. Malicious code protection locations should include (but not be limited to) items such as: workstations, mobile devices, and network appliances (I.e., firewalls and switches) *[a].*

Once the locations that require protection are identified, the organization will need to ensure that **Microsoft Defender Antivirus** is configured to conduct system scans on all devices enrolled using **Microsoft Intune.** The organization will also need to configure **Microsoft Defender Antivirus** to enable *always-on protection* which allows the solution to conduct real-time scans of the environment. This includes when USB devices and other external components are introduced to any asset, files are downloaded, or emails containing attachments are received [b]. **Exchange Online Protection** acts as an additional layer of defense, conducting real-time scans of communications to prevent spam, malware, and other email threats.

Microsoft technical reference documentation:

Enabling Microsoft Defender Antivirus "Always-on" protection

Scheduling a scan with Microsoft Defender Antivirus

Enabling antivirus policies on devices managed with Intune

Overview of Exchange online protection

SI. L1-3.14.4 - Update Malicious Code Protection

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

Determination statement:

[a] malicious code protection mechanisms are updated when new releases are available

Control summary:

The organization must ensure that the solution which provides protections to their environment from malicious content is updated when new threat signatures and virus definitions are available. Additionally, the organization will need to apply the updates to the antivirus solution on all devices which it is deployed.

Microsoft 365 licensing needed:

Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Microsoft Defender for Endpoint- Microsoft Defender for Endpoint Plan 1, Microsoft Defender Antivirus
- Microsoft Intune

How to implement:

Microsoft continually updates (every 2 hours) security intelligence in antimalware products to cover the latest threats and to constantly tweak detection logic, enhancing the ability of **Microsoft Defender Antivirus** and other Microsoft antimalware solutions to accurately identify threats. However, the organization must configure devices enrolled with **Microsoft Intune** to deploy automatic updates from **Microsoft Defender Antivirus** or implement a process to manually deploy the automatic updates to enrolled devices *[a].*

Microsoft technical reference documentation:

Security intelligence updates for Microsoft Defender Antivirus

Deploying updates with Intune

SI. L1-3.14.5 - System & File Scanning

Control language:

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

Assessment objective:

[a] the frequency for malicious code scans is defined

[b] malicious code scans are performed with the defined frequency

[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed

Control summary:

The organization should deploy an anti-virus / anti-malware solution to scan for and identify viruses on all devices. With this solution deployed the organization must configure the solution to scan for threats on a defined re-occurring frequency. The solution must also be configured to scan all external components (USB devices, portable storage) connected to any protected device; and scan any files or attachments prior to download.

Microsoft 365 licensing needed:
Microsoft 365 E3 licensing offers the following features to be leveraged to satisfy the requirements of this control:

- Microsoft Defender for Endpoint- Microsoft Defender for Endpoint Plan 1, Microsoft Defender Antivirus
- **Microsoft** Intune

How to implement using Microsoft 365:

The organization will need to determine the frequency at which its environment will be scanned for malicious code (computer viruses, worms, Trojan horses, logic bombs, spyware) and define that frequency in its documented policies and procedures *[a]*. Best

practice recommendations are to have the antivirus solution conduct a full system scan at least once daily. Additionally, the antivirus solution should conduct real-time scans on all emails, files, attachments, and downloads.

Microsoft Defender Antivirus will need to be configured to conduct systems scans on all devices enrolled using **Microsoft Intune** at the frequency defined by the organization *[b]*. Additionally, the organization will need to enable "always-on protection" Which enables **Microsoft Defender Antivirus** to conduct real-time scans of the environment; this includes when USB devices and other external components are introduced to endpoints, files are downloaded, or emails containing attachments are received *[c]*.

Microsoft technical reference documentation:

Enabling Microsoft Defender Antivirus "Always-on" protection

Scheduling a scan with Microsoft Defender Antivirus

Enabling antivirus policies on devices managed with Intune

Microsoft CMMC Blogs

- Accelerating CMMC compliance for Microsoft cloud
- Microsoft CMMC Acceleration Program Update
- The Microsoft 365 Government (GCC High) Conundrum - DIB Data Enclave vs Going All In
- Microsoft expands qualification of contractors for Government cloud offerings
- CMMC on Azure DevBlogs
- CMMC on Tech Community
- Understanding Compliance Between Commercial, Government and DoD Offerings

Microsoft CMMC Resources

- CMMC FAQ's
- CMMC 2.0 Model
- SECURING THE DEFENSE INDUSTRIAL BASE- CMMC 2.0

Microsoft CMMC Tools

• Microsoft Product Placemat for CMMC 2.0

Summit 7 CMMC Videos

- CMMC Videos
- When Will CMMC 2.0 Appear In Contracts?

Summit 7 CMMC Information Pages

- Security and Compliance For CMMC
- CMMC 2.0 For The Defense Industrial Base
- What Is CUI?

Summit 7 CMMC Downloads

- Microsoft 365 Licensing Guide
- A Guide to Microsoft 365 GCC vs GCC High

Summit 7 CMMC Blogs

- Do You Need GCC High For CMMC 2.0?
- Achieving CMMC 2.0 Compliance With a Shared Responsibility Model