Managing MSP Responsibilities for CMMC

Ryan Bonner

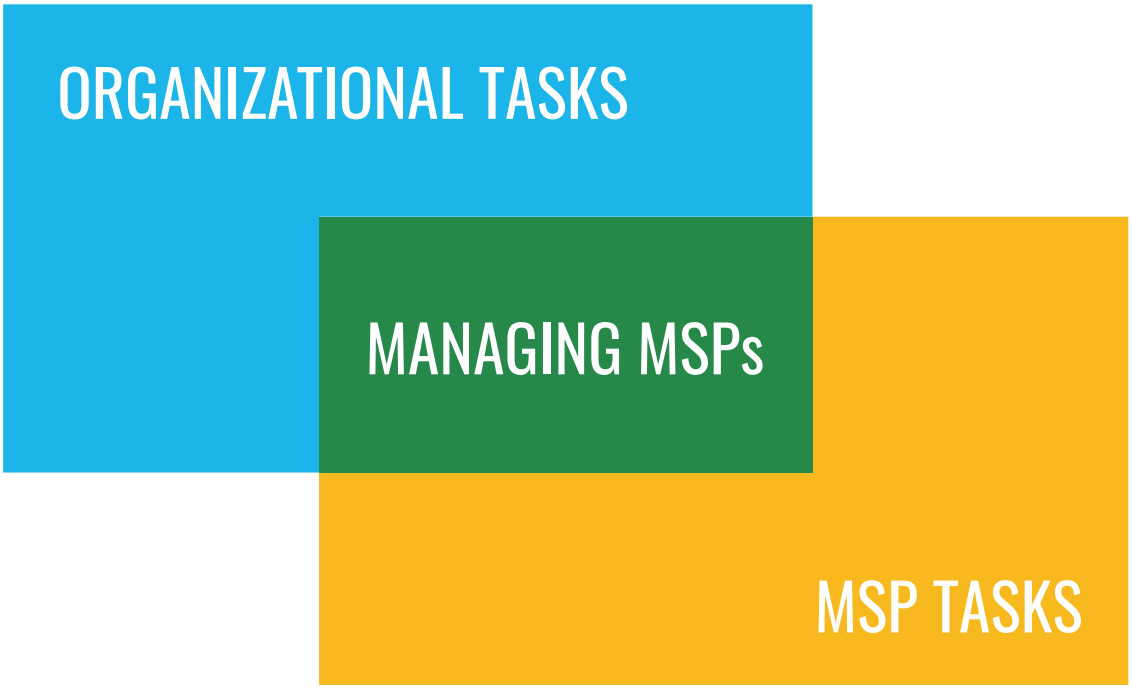
Becky Steck

DEFCERT

DEFCERT

Introduction

Working with a managed service provider (MSP) can significantly increase an organization's bandwidth for CMMC implementations. However, most organizations seeking certification (OSCs) don't have a clear picture of who does what to achieve compliance. Managing the overlap between organizational needs and an MSP's service capabilities is a critical skill all organizations must develop to make measurable progress and comply more quickly than their government contracting peers.



The Process

Organizations can manage their MSP's responsibilities during CMMC implementations by taking the following steps as part of a process designed for communication and accountability:

1. Separate Governance and Performance Objectives
2. Pre-Satisfy Governance Objectives
3. Determine Asset Capabilities
4. Describe the Work
5. Assign Responsibilities

STEP 1: SEPARATE GOVERNANCE AND PERFORMANCE OBJECTIVES

Each CMMC practice has one or more assessment objectives, used by internal and third-party assessors to validate whether the CMMC practice is fully implemented. Here's an example:

CMMC PRACTICE	ASSESSMENT OBJECTIVES
IA.L2-3.5.7 – Password Complexity Enforce a minimum password complexity and change of characters when new passwords are created.	[a] password complexity requirements are defined.
	[b] password change of character requirements are defined.
	[c] minimum password complexity requirements as defined are enforced when new passwords are created.
	[d] minimum password change of character requirements as defined are enforced when new passwords are created.

Assessment objectives take two forms: *governance objectives* and *performance objectives*. Governance objectives use "non-functional" language like *established, defined,* and *specified*. These objectives are often documented in a policy, standard, or system specification. Performance objectives use "functional" language like *enforced, limited*, and *controlled*.

Separating Governance and Performance Objectives

Divide governance and performance objectives, matching governance objectives (left column) with the performance objectives they relate to (right column):

GOVERNANCE OBJECTIVES	PERFORMANCE OBJECTIVES
[a] password complexity requirements are defined.	[c] minimum password complexity requirements as defined are enforced when new passwords are created.
[b] password change of character requirements are defined.	[d] minimum password change of character requirements as defined are enforced when new passwords are created.

STEP 2: PRE-SATISFY GOVERNANCE OBJECTIVES

Determine your own definitions, specifications, and measures of performance so that service providers' expectations are clear and manageable. Here are some example specifications (adapted from NIST SP 800-63B) designed to pre-satisfy the governance objectives for IA.L2-3.5.7:

GOVERNANCE OBJECTIVES	SPECIFICATIONS
[a] password complexity requirements are defined.	• Memorized secrets (passwords) must be at least 8 characters in length.
[b] password change of character requirements are defined.	• Systems must force a change if there is evidence of compromise of the authenticator. • At least one character of the password must change. • The system must compare the password against a list that contains values known to be commonly-used, expected, or compromised.

Documenting Governance Specifications

Communicate specifications to MSPs in writing. Policies are commonly used to convey rules or guidelines for day-to-day business operations. However, MSPs benefit from even more precise documents, such as a system policy, measurable standard, or system specification.

You can pre-satisfy the governance objectives above through the following actions:

- Create a password standard
- Review the password standard
- Approve the password standard
- Disseminate the password standard

STEP 3: DETERMINE ASSET CAPABILITIES

With governance objectives pre-satisfied, our next step is to identify the assets that are capable of satisfying our performance objectives. Three common asset types can provide protections for information assets: *people, technology,* and *facilities*.

Identify Which Assets Satisfy Performance Objectives

Using our three asset categories (people, technology, facilities), select the assets you expect to contribute toward satisfying each performance objective for IA.L2-3.5.7:

OBJECTIVE	PEOPLE	TECHNOLOGY	FACILITIES
[c] minimum password complexity requirements as defined are enforced when new passwords are created.	✓	✓	
[d] minimum password change of character requirements as defined are enforced when new passwords are created.	✓	✓	

Define Technology Assets

It's critical to involve your MSP during this step. Managed service providers are very familiar with the specific technologies, features, and capabilities they utilize (or could utilize) in your environment. Work with your MSP to identify the current and future technologies you will use.

OBJECTIVE	PEOPLE	TECHNOLOGY	FACILITIES
[c] minimum password complexity requirements as defined are enforced when new passwords are created.	✓	Active Directory	
[d] minimum password change of character requirements as defined are enforced when new passwords are created.	✓	Azure AD Password Protection	

STEP 4: DESCRIBE THE WORK

Once governance specifications and asset capabilities are identified, it's time to complete the most important step: describing the actions necessary to satisfy our performance objectives.

Actions can be described using simple verb/noun combinations ("approve change" or "install software"). These descriptions provide just enough detail to assign each action to the right people, roles, or teams. Here are some example actions:

OBJECTIVE	ACTION
[c] minimum password complexity requirements as defined are enforced when new passwords are created.	Review the password standard
	Configure the default domain password policy
	Install Azure AD Password Protection DC agent
[d] minimum password change of character requirements as defined are enforced when new passwords are created.	Enable self-service password reset
	Generate new passwords using a password manager
	Review password manager alerts for compromised or reused passwords

These actions serve to document "what" needs to happen, but don't go so far as to describe "how"- it's just enough information to allow us to assign each action to a responsible party.

Assign Frequencies for Performing Each Action

Finally, document how often each action must be performed. Some actions are a one-time activity completed during implementation ("as needed"), while others are part of an ongoing program.

ACTIONS	FREQUENCY
Review the password standard	Annually
Configure default domain password policy	As needed
Install Azure AD Password Protection DC agent	As needed

STEP 5: ASSIGN RESPONSIBILITIES

Responsibility doesn't exist in a vacuum. If you assign responsibility to an MSP with no expectations (accountability), guidance (consulting), or a reporting chain (informing all parties involved), your organization will be disappointed in external service provider performance.

Creating a RACI Matrix identifies who is **R**esponsible for an action, **A**ccountable for outcomes, **C**onsulted with for feedback and input, and **I**nformed of progress and results. Here's an example RACI Matrix for the actions we developed in Steps 2 and 4:

ACTIONS	CISO	SYSTEM OWNER	SYSTEM ADMIN	MSP
Create a password standard	I	A	R	C
Approve the password standard	R	I	I	I
Review the password standard	R	R	R	R
Configure default domain password policy	I	A	C	R
Install Azure AD Password Protection DC agent	I	A	R	C
Enable self-service password reset	I	A	C	R
Generate new password using password manager	R	R	R	R
Review password manager alerts for compromised or reused passwords	R	R	R	R

Documenting the responsibilities for each action allows you to quickly see where progress is stalled, and with whom. It also allows organizations to identify when individuals or teams are assigned more work than they can handle in the foreseeable future.

Bring it All Together

Once you have created your RACI Matrix, you can append the asset categories from Step 3 to create a clear and concise table of actions, owners, and associated assets. This artifact provides a clear playbook for all stakeholders across your business and your MSP, taking the guesswork out of implementing the CMMC program.

ACTIONS	FREQUENCY	CISO	SYSTEM OWNER	SYSTEM ADMIN	MSP	PEOPLE	TECH	FACILITIES
Create a password standard	As needed	I	A	R	C	System Admin	-	-
Approve the password standard	As needed	R	I	I	I	CISO	-	-
Review the password standard	Annually	R	R	R	R	All Personnel	-	-
Configure default domain password policy	As needed	I	A	C	R	MSP	Active Directory	-
Install Azure AD Password Protection DC agent	As needed	I	A	R	C	System Admin	Azure AD Password Protection	-
Enable self-service password reset	As needed	I	A	C	R	MSP	Azure AD	-
Generate new password using password manager	As needed	R	R	R	R	All Personnel	Password Manager	-
Review password manager alerts for compromised or reused passwords	Weekly	R	R	R	R	All Personnel	Password Manager	-

About DEFCERT

DEFCERT discovers and delivers new ways for the defense industrial base (DIB) and government contractors to meet their contractual and regulatory obligations for data protection. These efforts include compliance with DFARS safeguarding clauses, implementation of NIST special publications, and future assessment under the Cybersecurity Maturity Model Certification (CMMC).

DEFCERT primarily works with defense contractors, manufacturers, economic development organizations, managed IT service providers, and technology companies offering solutions to the defense industrial base.

2155 Jackson Ave
Ann Arbor, MI 48103

info@defcert.com

DEFCERT