CMMC 2.0 Shared Responsibility Matrix - MSP SAMPLE

Practice Area	Practice	Practice ID	Practice	AO ID	Assessment Objective	MSP Responsibility	Customer Responsibility
Access Control							
	Authorized Access Control	**AC.L1-3.1.1**	**Limit Information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).**				
		AC.L1-3.1.1		**a**	Authorized users are identified.	Identify named MSP users with access to environment.	Identify all authorized users other than MSP team.
		AC.L1-3.1.1		**b**	Processes acting on behalf of authorized users are identified.	Full responsibility	
		AC.L1-3.1.1		**c**	Devices (and other systems) authorized to connect to the system are identified.	MSP is responsbile for presenting lists of IP's on the network for customer identification and authorization.	Customer is responsible for determining what devices are authorized to access the network.
		AC.L1-3.1.1		**d**	System access is limited to authorized users.	Full responsibility	
		AC.L1-3.1.1		**e**	System access is limited to processes acting on behalf of authorized users.	Full responsibility	
		AC.L1-3.1.1		**f**	System access is limited to authorized devices (including other systems).	Full responsibility	
	Transaction & Function Control	**AC.L1-3.1.2**	**Limit information system access to the types of transactions and functions that authorized users are permitted to execute.**				
				a	The types of transactions and functions that authorized users are permitted to execute are defined.		Full responsibility
				b	System access is limited to the defined types of transactions and functions for authorized users.	MSP is responsible for limiting the types of transactions and functions that are customer defined on the systems they manage.	
	Control CUI Flow	**AC.L2-3.1.3**	**Control the flow of CUI in accordance with approved authorizations.**				
				a	Information flow control policies are defined.		Full responsibility
				b	Methods and enforcement mechanisms for controlling the flow of CUI are defined.		Full responsibility
				c	Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.		Full responsibility
				d	Authorizations for controlling the flow of CUI are defined.		Full responsibility
				e	Approved authorizations for controlling the flow of CUI are enforced.		Full responsibility
	Separation of Duties	**AC.L2-3.1.4**	**Separate the duties of individuals to reduce the risk of malevolent activity without collusion.**				
				a	The duties of individuals requiring separation are defined.	MSP identifies roles, individuals, and informs customer	

CMMC 2.0 Shared Responsibility Matrix - MSP SAMPLE

Configuration and Management							
	System Change Management	**CM.L2-3.4.3**	**Track, review, approve, or disapprove, and log changes to organizational systems.**				
				a	Changes to the system are tracked.	Full responsibility	
				b	Changes to the system are reviewed.	MSP is responsible for assuring change management process is followed.	Customer responsibility to respond when change process requires that a request is reviewed and approved by an internal decision maker
				c	Changes to the system are approved or disapproved.	MSP is responsible for assuring change management process is followed.	Customer responsibility to respond when change process requires that a request is reviewed and approved by an internal decision maker
				d	Changes to the system are logged.	MSP is responsible for assuring change management process is followed.	
	Security Impact Analysis	**CM.L2-3.4.4**	**Analyze the security impact of changes prior to implementation.**				
				a	The security impact of changes to the system is analyzed prior to implementation.	MSP is responsible for assuring change management process is followed for equipment under management.	Customer is responsible for assuring change management process is followed for equipment they management.
	Access Restrictions for Change	**CM.L2-3.4.5**	**Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.**				
				a	Physical access restrictions associated with changes to the system are defined.		Full responsibility
				b	Physical access restrictions associated with changes to the system are documented.		Full responsibility
				c	Physical access restrictions associated with changes to the system are approved.		Full responsibility
				d	Physical access restrictions associated with changes to the system are enforced.		Full responsibility
				e	Logical access restrictions associated with changes to the system are defined.	MSP is responsible for defining, documenting, approving, and enforcing the logical access restrictions	
				f	Logical access restrictions associated with changes to the system are documented.	MSP is responsible for defining, documenting, approving, and enforcing the logical access restrictions	
				g	Logical access restrictions associated with changes to the system are approved.	MSP is responsible for defining, documenting, approving, and enforcing the logical access restrictions	