

FedRAMP Moderate Control Implementation Summary (CIS) Worksheet

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
AC-1(a)	X							X				
AC-1(b)	X							X				
AC-1(c)	X							X				
AC-2(a)	X						X		X	X	X	X
AC-2(b)	X						X		X	X	X	X
AC-2(c)	X						X		X	X	X	X
AC-2(d)	X						X		X	X	X	X
AC-2(e)	X						X		X	X	X	X
AC-2(f)	X						X		X	X	X	X
AC-2(g)	X						X		X	X	X	X
AC-2(h)	X						X		X	X	X	X
AC-2(i)	X						X		X	X	X	X
AC-2(j)	X						X		X	X	X	X
AC-2(k)	X						X		X	X	X	X
AC-2(l)	X						X		X	X	X	X
AC-2(1)	X						X		X	X	X	X
AC-2(2)	X						X		X	X	X	X
AC-2(3)(a)	X						X		X	X	X	X
AC-2(3)(b)	X						X	X		X	X	X
AC-2(3)(c)	X						X		X	X	X	X
AC-2(3)(d)	X						X	X		X	X	X
AC-2(4)	X						X		X	X	X	X
AC-2(5)	X						X		X	X	X	X
AC-2(7)(a)	X						X		X	X	X	X
AC-2(7)(b)	X						X		X	X	X	X
AC-2(7)(c)	X						X		X	X	X	X
AC-2(7)(d)	X						X		X	X	X	X
AC-2(9)	X						X		X	X	X	X
AC-2(12)(a)	X						X		X	X	X	X
AC-2(12)(b)	X						X		X	X	X	X
AC-2(13)	X						X		X	X	X	X
AC-3	X						X	X		X	X	X
AC-4	X						X		X	X	X	X
AC-4(21)	X						X		X	X	X	X
AC-5(a)	X						X		X	X	X	X
AC-5(b)	X						X		X	X	X	X
AC-6	X							X		X	X	X
AC-6(1)(a)	X							X		X	X	X
AC-6(1)(b)	X							X		X	X	X
AC-6(2)	X							X		X	X	X
AC-6(5)	X							X	X	X	X	X
AC-6(7)(a)	X						X		X	X	X	X
AC-6(7)(b)	X						X		X	X	X	X
AC-6(9)	X						X		X	X	X	X
AC-6(10)	X						X		X	X	X	X
AC-7(a)	X						X		X	X	X	X
AC-7(b)	X						X		X	X	X	X
AC-8(a)	X						X		X	X	X	X
AC-8(b)	X						X		X	X	X	X
AC-8(c)	X						X		X	X	X	X
AC-11(a)	X						X		X	X	X	X
AC-11(b)	X						X		X	X	X	X
AC-11(1)	X						X		X	X	X	X
AC-12	X						X	X	X	X	X	X
AC-14(a)	X						X		X	X	X	X
AC-14(b)	X						X		X	X	X	X
AC-17(a)	X							X	X	X	X	X

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
AC-17(b)	X							X	X		X	X
AC-17(1)	X						X			X	X	X
AC-17(2)	X						X					X
AC-17(3)	X						X					X
AC-17(4)(a)	X						X					X
AC-17(4)(b)	X						X					X
AC-18(a)	X						X					X
AC-18(b)	X						X					X
AC-18(1)	X						X					X
AC-18(3)	X						X					X
AC-19(a)	X						X					X
AC-19(b)	X						X					X
AC-19(5)	X						X					X
AC-20(a)	X						X		X		X	
AC-20(b)	X						X		X		X	
AC-20(1)(a)	X						X		X		X	
AC-20(1)(b)	X						X		X		X	
AC-20(2)	X						X					X
AC-21(a)	X						X		X		X	
AC-21(b)	X						X		X		X	
AC-22(a)	X						X					
AC-22(b)	X						X					
AC-22(c)	X						X					
AC-22(d)	X						X					
AT-1(a)	X							X				
AT-1(b)	X							X				
AT-1(c)	X							X				
AT-2(a)	X					X			X		X	
AT-2(b)	X					X			X		X	
AT-2(c)	X					X			X		X	
AT-2(d)	X					X			X		X	
AT-2(2)	X					X			X		X	
AT-2(3)	X					X			X		X	
AT-3(a)	X					X			X		X	
AT-3(b)	X					X			X		X	
AT-3(c)	X					X			X		X	
AT-4(a)	X					X			X		X	
AT-4(b)	X					X			X		X	
AU-1(a)	X							X				
AU-1(b)	X							X				
AU-1(c)	X							X				
AU-2(a)	X						X					
AU-2(b)	X						X					
AU-2(c)	X						X					
AU-2(d)	X						X					
AU-2(e)	X						X					
AU-3(a)	X						X					X
AU-3(b)	X						X					X
AU-3(c)	X						X					X
AU-3(d)	X						X					X
AU-3(e)	X						X					X
AU-3(f)	X						X					X
AU-3(1)	X						X					
AU-4	X						X		X		X	X
AU-5(a)	X						X		X		X	
AU-5(b)	X						X		X		X	
AU-6(a)	X						X		X		X	
AU-6(b)	X						X		X		X	
AU-6(c)	X						X		X		X	
AU-6(1)	X						X		X		X	

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
AU-6(3)	X						X		X	X	X	
AU-7(a)	X						X					
AU-7(b)	X						X					
AU-7(1)	X						X					
AU-8(a)	X						X					X
AU-8(b)	X						X					X
AU-9(a)	X						X					
AU-9(b)	X						X					
AU-9(4)	X						X					
AU-11	X						X					
AU-12(a)	X						X	X	X	X	X	X
AU-12(b)	X						X	X	X	X	X	X
AU-12(c)	X						X	X	X	X	X	X
CA-1(a)	X							X				
CA-1(b)	X							X				
CA-1(c)	X							X				
CA-2(a)	X						X					
CA-2(b)	X						X					
CA-2(c)	X						X					
CA-2(d)	X						X					
CA-2(e)	X						X					
CA-2(f)	X						X					
CA-2(1)	X						X					
CA-2(3)	X						X					
CA-3(a)	X						X					
CA-3(b)	X						X					
CA-3(c)	X						X					
CA-5(a)	X						X					
CA-5(b)	X						X					
CA-6(a)	X						X					
CA-6(b)	X						X					
CA-6(c)	X						X					
CA-6(d)	X						X					
CA-6(e)	X						X					
CA-7(a)	X						X					
CA-7(b)	X						X					
CA-7(c)	X						X					
CA-7(d)	X						X					
CA-7(e)	X						X					
CA-7(f)	X						X					
CA-7(g)	X						X					
CA-7(1)	X						X					
CA-7(4)(a)	X						X					
CA-7(4)(b)	X						X					
CA-7(4)(c)	X						X					
CA-8	X						X					
CA-8(1)	X						X					
CA-8(2)	X						X					
CA-9(a)	X						X					
CA-9(b)	X						X					
CA-9(c)	X						X					
CA-9(d)	X						X					
CM-1(a)	X							X				
CM-1(b)	X							X				
CM-1(c)	X							X				
CM-2(a)	X						X					
CM-2(b)	X						X					
CM-2(2)	X						X					X
CM-2(3)	X						X					X
CM-2(7)(a)	X						X					X

Control ID	Implementation Status					Control Origination							
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization	
CM-2(7)(b)	X						X					X	
CM-3(a)				X				X					
CM-3(b)				X				X					
CM-3(c)				X				X					
CM-3(d)				X				X					
CM-3(e)				X				X					
CM-3(f)				X				X					
CM-3(g)				X				X					
CM-3(2)	X							X					
CM-3(4)	X					X							
CM-4	X						X						
CM-4(2)	X						X						
CM-5	X						X					X	
CM-5(1)(a)	X						X					X	
CM-5(1)(b)	X						X					X	
CM-5(5)(a)	X						X					X	
CM-5(5)(b)	X						X					X	
CM-6(a)	X						X					X	
CM-6(b)	X						X					X	
CM-6(c)	X						X					X	
CM-6(d)	X						X					X	
CM-6(1)	X						X						
CM-7(a)	X						X						
CM-7(b)	X						X						
CM-7(1)(a)	X						X						
CM-7(1)(b)	X						X						
CM-7(2)	X						X	X	X	X			
CM-7(5)(a)	X						X	X	X	X			
CM-7(5)(b)	X						X	X	X	X			
CM-7(5)(c)	X						X	X	X	X			
CM-8(a)	X						X						
CM-8(b)	X						X						
CM-8(1)	X						X						
CM-8(3)(a)	X							X	X	X			
CM-8(3)(b)	X							X	X	X			
CM-9(a)	X						X						
CM-9(b)	X						X						
CM-9(c)	X						X						
CM-9(d)	X						X						
CM-9(e)	X						X						
CM-10(a)	X						X						
CM-10(b)	X						X						
CM-10(c)	X						X						
CM-11(a)	X						X	X	X	X			
CM-11(b)	X						X	X	X	X			
CM-11(c)	X						X	X	X	X			
CM-12(a)	X						X						
CM-12(b)	X						X						
CM-12(c)	X						X						
CM-12(1)			X				X						
CP-1(a)	X							X					
CP-1(b)	X							X					
CP-1(c)	X							X					
CP-2(a)	X						X						
CP-2(b)	X						X						
CP-2(c)	X						X						
CP-2(d)	X						X						
CP-2(e)	X						X						
CP-2(f)	X						X						
CP-2(g)	X						X						

Control ID	Implementation Status					Control Origination							
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization	
CP-2(h)	X						X						
CP-2(1)	X						X						
CP-2(3)	X						X		X			X	
CP-2(8)	X						X						
CP-3(a)	X						X						
CP-3(b)	X						X						
CP-4(a)	X						X						
CP-4(b)	X						X						
CP-4(c)	X						X						
CP-4(1)	X						X						
CP-6(a)	X						X		X		X	X	
CP-6(b)	X						X		X		X	X	
CP-6(1)	X						X		X		X	X	
CP-6(3)	X						X		X		X	X	
CP-7(a)	X						X		X		X	X	
CP-7(b)	X						X		X		X	X	
CP-7(c)	X						X		X		X	X	
CP-7(1)	X						X		X		X	X	
CP-7(2)	X						X		X		X	X	
CP-7(3)	X						X		X		X	X	
CP-8	X						X		X		X	X	
CP-8(1)(a)	X						X		X		X	X	
CP-8(1)(b)	X						X		X		X	X	
CP-8(2)	X						X		X		X	X	
CP-9(a)	X						X		X		X	X	
CP-9(b)	X						X		X		X	X	
CP-9(c)	X						X		X		X	X	
CP-9(d)	X						X		X		X	X	
CP-9(1)	X						X		X		X	X	
CP-9(8)	X						X		X		X	X	
CP-10	X						X		X		X	X	
CP-10(2)	X						X		X		X	X	
IA-1(a)	X							X					
IA-1(b)	X							X					
IA-1(c)	X							X					
IA-2	X						X		X		X	X	
IA-2(1)	X						X		X		X	X	
IA-2(2)	X						X		X		X	X	
IA-2(5)	X						X		X		X	X	
IA-2(6)(a)	X						X		X		X	X	
IA-2(6)(b)	X						X		X		X	X	
IA-2(8)	X						X		X		X	X	
IA-2(12)	X						X		X		X	X	
IA-3	X						X		X		X	X	
IA-4(a)	X						X		X		X	X	
IA-4(b)	X						X		X		X	X	
IA-4(c)	X						X		X		X	X	
IA-4(d)	X						X		X		X	X	
IA-4(4)	X						X		X		X	X	
IA-5(a)	X						X		X		X	X	
IA-5(b)	X						X		X		X	X	
IA-5(c)	X						X		X		X	X	
IA-5(d)	X						X		X		X	X	
IA-5(e)	X						X		X		X	X	
IA-5(f)	X						X		X		X	X	
IA-5(g)	X						X		X		X	X	
IA-5(h)	X						X		X		X	X	
IA-5(i)	X						X		X		X	X	
IA-5(1)(a)	X						X		X		X	X	
IA-5(1)(b)	X						X		X		X	X	

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
IA-5(1)(c)	X						X		X	X	X	X
IA-5(1)(d)	X						X		X	X	X	X
IA-5(1)(e)	X						X		X	X	X	X
IA-5(1)(f)	X						X		X	X	X	X
IA-5(1)(g)	X						X		X	X	X	X
IA-5(1)(h)	X						X		X	X	X	X
IA-5(2)(a)	X						X					
IA-5(2)(b)	X						X					
IA-5(6)	X						X		X	X		
IA-5(7)	X						X		X	X		
IA-6	X						X		X	X		X
IA-7	X						X		X	X		X
IA-8	X						X		X	X		
IA-8(1)	X						X		X	X		
IA-8(2)(a)	X								X	X		
IA-8(2)(b)	X								X	X		
IA-8(4)	X								X			
IA-11	X					X						
IA-12(a)	X							X				
IA-12(b)	X							X				
IA-12(c)	X							X				
IA-12(2)	X							X				
IA-12(3)	X							X				
IA-12(5)	X					X						
IR-1(a)	X							X				
IR-1(b)	X							X				
IR-1(c)	X							X				
IR-2(a)	X						X					
IR-2(b)	X						X					
IR-3	X						X					
IR-3(2)	X						X	X				
IR-4(a)	X						X					
IR-4(b)	X						X					
IR-4(c)	X						X					
IR-4(d)	X						X					
IR-4(1)	X							X				
IR-5	X						X	X				
IR-6(a)	X						X		X	X		
IR-6(b)	X						X		X	X		
IR-6(1)	X						X					
IR-6(3)	X						X	X				
IR-7	X						X	X				
IR-7(1)	X						X	X				
IR-8(a)	X						X	X				
IR-8(b)	X						X	X				
IR-8(c)	X						X	X				
IR-8(d)	X						X	X				
IR-8(e)	X						X	X				
IR-9(a)	X						X	X				
IR-9(b)	X						X	X				
IR-9(c)	X						X	X				
IR-9(d)	X						X	X				
IR-9(e)	X						X	X				
IR-9(f)	X						X	X				
IR-9(g)	X						X	X				
IR-9(2)	X						X					
IR-9(3)	X						X					
IR-9(4)	X						X					
MA-1(a)	X							X				
MA-1(b)	X							X				

Control ID	Implementation Status					Control Origination							
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization	
PE-6(c)	X											X	
PE-6(1)	X											X	
PE-8(a)	X											X	
PE-8(b)	X											X	
PE-8(c)	X											X	
PE-9	X											X	
PE-10(a)	X											X	
PE-10(b)	X											X	
PE-10(c)	X											X	
PE-11	X											X	
PE-12	X											X	
PE-13	X											X	
PE-13(1)	X											X	
PE-13(2)(a)	X											X	
PE-13(2)(b)	X											X	
PE-14(a)	X											X	
PE-14(b)	X											X	
PE-15	X											X	
PE-16(a)	X											X	
PE-16(b)	X											X	
PE-17(a)	X											X	
PE-17(b)	X											X	
PE-17(c)	X											X	
PE-17(d)	X											X	
PL-1(a)	X							X					
PL-1(b)	X							X					
PL-1(c)	X							X					
PL-2(a)	X						X						
PL-2(b)	X						X						
PL-2(c)	X						X						
PL-2(d)	X						X						
PL-2(e)	X						X						
PL-4(a)	X							X					
PL-4(b)	X							X					
PL-4(c)	X							X					
PL-4(d)	X							X					
PL-4(1)(a)	X							X					
PL-4(1)(b)	X							X					
PL-4(1)(c)	X							X					
PL-8(a)	X						X						
PL-8(b)	X						X						
PL-8(c)	X						X						
PL-10	X						X						
PL-11	X						X						
PS-1(a)	X							X					
PS-1(b)	X							X					
PS-1(c)	X							X					
PS-2(a)	X							X					
PS-2(b)	X							X					
PS-2(c)	X							X					
PS-3(a)	X							X					
PS-3(b)	X							X					
PS-3(3)(a)	X							X					
PS-3(3)(b)	X							X					
PS-4(a)	X					X							
PS-4(b)	X					X							
PS-4(c)	X					X							
PS-4(d)	X					X							
PS-4(e)	X					X							
PS-5(a)	X					X							

Control ID	Implementation Status					Control Origination							
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization	
PS-5(b)	X					X							
PS-5(c)	X					X							
PS-5(d)	X					X							
PS-6(a)	X							X					
PS-6(b)	X							X					
PS-6(c)	X							X					
PS-7(a)	X					X							
PS-7(b)	X					X							
PS-7(c)	X					X							
PS-7(d)	X					X							
PS-7(e)	X					X							
PS-8(a)	X					X							
PS-8(b)	X					X							
PS-9	X					X							
RA-1(a)	X							X					
RA-1(b)	X							X					
RA-1(c)	X							X					
RA-2(a)	X						X						
RA-2(b)	X						X						
RA-2(c)	X						X						
RA-3(a)	X						X						
RA-3(b)	X						X						
RA-3(c)	X						X						
RA-3(d)	X						X						
RA-3(e)	X						X						
RA-3(f)	X						X						
RA-3(1)(a)	X						X						
RA-3(1)(b)	X						X						
RA-5(a)	X						X				X		
RA-5(b)	X						X				X		
RA-5(c)	X						X				X		
RA-5(d)	X						X				X		
RA-5(e)	X						X				X		
RA-5(f)	X						X				X		
RA-5(2)	X						X				X		
RA-5(3)	X						X				X		
RA-5(5)	X						X				X		
RA-5(11)	X						X						
RA-7	X						X						
RA-9	X						X						
SA-1(a)	X							X					
SA-1(b)	X							X					
SA-1(c)	X							X					
SA-2(a)	X						X						
SA-2(b)	X						X						
SA-2(c)	X						X						
SA-3(a)	X						X						
SA-3(b)	X						X						
SA-3(c)	X						X						
SA-3(d)	X						X						
SA-4(a)	X							X					
SA-4(b)	X							X					
SA-4(c)	X							X					
SA-4(d)	X							X					
SA-4(e)	X							X					
SA-4(f)	X							X					
SA-4(g)	X							X					
SA-4(h)	X							X					
SA-4(i)	X							X					
SA-4(1)	X						X						

Control ID	Implementation Status					Control Origination							
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization	
SA-4(2)	X						X						
SA-4(9)	X						X						
SA-4(10)	X									X			
SA-5(a)	X						X						
SA-5(b)	X						X						
SA-5(c)	X						X						
SA-5(d)	X						X						
SA-8	X						X						
SA-9(a)	X						X						
SA-9(b)	X						X						
SA-9(c)	X						X						
SA-9(1)(a)	X						X						
SA-9(1)(b)	X						X						
SA-9(2)	X						X						
SA-9(5)	X						X					X	
SA-10(a)	X						X						
SA-10(b)	X						X						
SA-10(c)	X						X						
SA-10(d)	X						X						
SA-10(e)	X						X						
SA-11(a)	X						X						
SA-11(b)	X						X						
SA-11(c)	X						X						
SA-11(d)	X						X						
SA-11(e)	X						X						
SA-11(1)	X						X						
SA-11(2)(a)	X						X						
SA-11(2)(b)	X						X						
SA-11(2)(c)	X						X						
SA-11(2)(d)	X						X						
SA-15(a)	X						X						
SA-15(b)	X						X						
SA-15(3)(a)	X						X						
SA-15(3)(b)	X						X						
SA-22(a)	X						X						
SA-22(b)	X						X						
SC-1(a)	X							X					
SC-1(b)	X							X					
SC-1(c)	X							X					
SC-2	X						X						
SC-4	X						X						
SC-5(a)	X											X	
SC-5(b)	X											X	
SC-7(a)	X						X		X	X		X	
SC-7(b)	X						X		X	X		X	
SC-7(c)	X						X		X	X		X	
SC-7(3)	X						X		X	X		X	
SC-7(4)(a)	X						X		X	X		X	
SC-7(4)(b)	X						X		X	X		X	
SC-7(4)(c)	X						X		X	X		X	
SC-7(4)(d)	X						X		X	X		X	
SC-7(4)(e)	X						X		X	X		X	
SC-7(4)(f)	X						X		X	X		X	
SC-7(4)(g)	X						X		X	X		X	
SC-7(4)(h)	X						X		X	X		X	
SC-7(5)	X						X					X	
SC-7(7)	X					X							
SC-7(8)	X			X			X					X	
SC-7(12)	X						X						
SC-7(18)	X						X					X	

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
SC-8	X						X					X
SC-8(1)	X						X					
SC-10	X						X		X	X	X	X
SC-12	X						X					
SC-13(a)	X						X		X	X	X	X
SC-13(b)	X						X		X	X	X	X
SC-15(a)	X						X					
SC-15(b)	X						X					
SC-17(a)	X						X					
SC-17(b)	X						X					
SC-18(a)	X						X					
SC-18(b)	X						X					
SC-20(a)	X						X					
SC-20(b)	X						X					
SC-21	X						X		X		X	X
SC-22	X						X					X
SC-23	X						X					
SC-28	X						X			X	X	X
SC-28(1)	X						X		X	X	X	X
SC-39	X						X					
SC-45	X						X					
SC-45(1)(a)	X						X					X
SC-45(1)(b)	X						X					X
SI-1(a)	X							X				
SI-1(b)	X							X				
SI-1(c)	X							X				
SI-2(a)	X						X					
SI-2(b)	X						X					
SI-2(c)	X						X					
SI-2(d)	X						X					
SI-2(2)	X						X					
SI-2(3)(a)	X						X					
SI-2(3)(b)	X						X					
SI-3(a)	X						X		X	X		
SI-3(b)	X						X		X	X		
SI-3(c)	X						X		X	X		
SI-3(d)	X						X		X	X		
SI-4(a)	X						X		X	X		X
SI-4(b)	X						X		X	X		X
SI-4(c)	X						X		X	X		X
SI-4(d)	X						X		X	X		X
SI-4(e)	X						X		X	X		X
SI-4(f)	X						X		X	X		X
SI-4(g)	X						X		X	X		X
SI-4(1)	X						X		X	X		
SI-4(2)	X						X		X	X		
SI-4(4)(a)	X						X		X	X		X
SI-4(4)(b)	X						X		X	X		X
SI-4(5)	X						X		X	X		
SI-4(16)	X						X		X	X		
SI-4(18)	X						X		X	X		
SI-4(23)	X						X					
SI-5(a)	X						X					
SI-5(b)	X						X					
SI-5(c)	X						X					
SI-5(d)	X						X					
SI-6(a)	X						X		X	X		
SI-6(b)	X						X		X	X		
SI-6(c)	X						X		X	X		
SI-6(d)	X						X		X	X		

FedRAMP Moderate Customer Responsibility Matrix (CRM) Worksheet

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-1(a)	Yes	
AC-1(b)	Yes	
AC-1(c)	Yes	
AC-2(a)	Yes	
AC-2(b)	Yes	
AC-2(c)	Yes	
AC-2(d)	Yes	
AC-2(e)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(f)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(g)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and monitoring the use of their accounts.
AC-2(h)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(i)	Yes	
AC-2(j)	Yes	
AC-2(k)	Yes	
AC-2(l)	Yes	
AC-2(1)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html).
		Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html).
		Customers are also responsible for permitting access of Databricks employees to their environment and for enforcing the access expiration (https://docs.databricks.com/administration-guide/workspace/workspace-access.html).
AC-2(2)	Partial	
AC-2(3)(a)	Yes	
AC-2(3)(b)	Yes	
AC-2(3)(c)	Yes	
AC-2(3)(d)	Partial	Customers are responsible for disabling their user's access to Databricks after a period of inactivity.
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and auditing the creation, modification, enabling, disabling, and removal of their accounts.
AC-2(4)	Partial	
AC-2(5)	Partial	Customers are responsible for initiating a session timeout within their identity provider.
		Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(7)(a)	Partial	
AC-2(7)(b)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(7)(c)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(7)(d)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(9)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(12)(a)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-2(12)(b)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and monitoring the use of their accounts
AC-2(13)	Yes	
AC-3	Partial	Customers are responsible for configuring their own identity provider.
		Customers are responsible for managing the networking of their AWS account. Customers are responsible for managing connections to/from their Databricks workspace including, but not limited to the following: IP access lists to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html) and mounting their data sources (https://docs.databricks.com/data/data-sources/index.html)
AC-4	Partial	
AC-4(21)	Yes	
AC-5(a)	Partial	Customers are responsible for managing their Databricks user's access including separating duties as appropriate. User Entitlements: https://docs.databricks.com/administration-guide/users-groups/users.html#manage-user-entitlements and Group Entitlements: https://docs.databricks.com/administration-guide/users-groups/groups.html#manage-a-groups-entitlements
AC-5(b)	Partial	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
		Customers are responsible for managing their Databricks user's access and employing the principle of least privilege. User Entitlements: https://docs.databricks.com/administration-guide/users-groups/users.html#manage-user-entitlements Group Entitlements: https://docs.databricks.com/administration-guide/users-groups/groups.html#manage-a-groups-entitlements
AC-6	Partial	
AC-6(1)(a)	Yes	
AC-6(1)(b)	Yes	
AC-6(2)	Yes	
AC-6(5)	Yes	
AC-6(7)(a)	Yes	
AC-6(7)(b)	Yes	
AC-6(9)	Yes	
AC-6(10)	Yes	
AC-7(a)	Partial	Customers are responsible for limiting the number of consecutive invalid logon attempts to the Databricks web application using their single sign-on solution.
AC-7(b)	Partial	Customers are responsible for locking accounts to the Databricks web application using their single sign-on solution.
AC-8(a)	Partial	Customers are responsible for configuring their single sign-on solution to display a system use notification prior to redirecting users to the Databricks web application.
AC-8(b)	Yes	
AC-8(c)	Yes	
AC-11(a)	Partial	guide/account-settings/audit-logs.html#configure-audit-log-delivery) and monitoring access to their Databricks workspace.
AC-11(b)	Partial	Customers are responsible for initiating a session timeout within their identity provider.
AC-11(1)	Partial	Customers are responsible for initiating a session timeout within their identity provider.
AC-12	Partial	Customers are responsible for initiating a session timeout within their identity provider.
AC-14(a)	Partial	Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html).
AC-14(b)	Partial	Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html).
AC-17(a)	Partial	Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html).
AC-17(b)	Partial	Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html).
AC-17(1)	Partial	guide/account-settings/audit-logs.html#configure-audit-log-delivery) and monitoring access to their Databricks workspace.
AC-17(2)	Yes	
AC-17(3)	Yes	
AC-17(4)(a)	Yes	
AC-17(4)(b)	Yes	
AC-18(a)	Yes	
AC-18(b)	Yes	
AC-18(1)	Yes	
AC-18(3)	Yes	
AC-19(a)	Yes	
AC-19(b)	Yes	
AC-19(5)	Yes	
		Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html). Customers are responsible for configuring their single sign-on solution (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for assigning users access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-20(a)	Partial	
AC-20(b)	Yes	
		Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html). Customers are responsible for configuring their single sign-on solution (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for assigning users access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
AC-20(1)(a)	Partial	
AC-20(1)(b)	Partial	Customers are responsible for mounting their data sources (https://docs.databricks.com/data/data-sources/index.html).
AC-20(2)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
		Customers are responsible for using Databricks workspace access controls (https://docs.databricks.com/security/access-control/workspace-acl.html) when sharing folders and notebooks. Customers are responsible for acting as a "Data Provider" when using Delta Sharing (https://docs.databricks.com/delta-sharing/recipient.html).
AC-21(a)	Partial	
		Customers are responsible for using Databricks workspace access controls (https://docs.databricks.com/security/access-control/workspace-acl.html) when sharing folders and notebooks. Customers are responsible for acting as a "Data Provider" when using Delta Sharing (https://docs.databricks.com/delta-sharing/recipient.html).
AC-21(b)	Partial	
AC-22(a)	Yes	
AC-22(b)	Yes	
AC-22(c)	Yes	
AC-22(d)	Yes	
AT-1(a)	Yes	
AT-1(b)	Yes	
AT-1(c)	Yes	
AT-2(a)	Partial	Customers are responsible for providing basic security awareness training to their users as part of the initial training for new users.
AT-2(b)	Partial	Customers are responsible for providing basic security awareness training to their users as part of the initial training for new users.
AT-2(c)	Partial	Customers are responsible for updating basic security awareness training to their users.
AT-2(d)	Partial	Customers are responsible for updating basic security awareness training to their users.
AT-2(2)	Partial	Customers are responsible for providing security awareness training on recognizing and reporting potential indicators of insider threat to their users.
AT-2(3)	Partial	Customers are responsible for incorporating training on social engineering and mining for their users.
AT-3(a)	Partial	Customers are responsible for providing role-based security training to their personnel with assigned security roles and responsibilities and updating it appropriately.
AT-3(b)	Partial	Customers are responsible for providing role-based security training to their personnel with assigned security roles and responsibilities and updating it appropriately.
AT-3(c)	Partial	Customers are responsible for providing role-based security training to their personnel with assigned security roles and responsibilities and updating it appropriately.
AT-4(a)	Partial	Customers are responsible for documenting, monitoring, and retaining security training records for their users.
AT-4(b)	Partial	Customers are responsible for documenting, monitoring, and retaining security training records for their users.
AU-1(a)	Yes	
AU-1(b)	Yes	
AU-1(c)	Yes	
AU-2(a)	Yes	
AU-2(b)	Yes	
AU-2(c)	Yes	
AU-2(d)	Yes	
AU-2(e)	Yes	
AU-3(a)	Yes	
AU-3(b)	Yes	
AU-3(c)	Yes	
AU-3(d)	Yes	
AU-3(e)	Yes	
AU-3(f)	Yes	
AU-3(1)	Yes	
AU-4	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and the capacity of these logs.
AU-5(a)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and the monitoring of these logs.
AU-5(b)	Partial	Customers are responsible configuring Databricks Audit Log Delivery
AU-6(a)	Yes	
AU-6(b)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and the monitoring of these logs.
AU-6(c)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and the monitoring of these logs.
AU-6(1)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and the monitoring of these logs.

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
AU-6(3)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and the monitoring of these logs.
AU-7(a)	Partial	
AU-7(b)	Yes	
AU-7(1)	Yes	
AU-8(a)	Yes	
AU-8(b)	Yes	
AU-9(a)	Yes	
AU-9(b)	Yes	
AU-9(4)	Yes	
AU-11	Yes	
AU-12(a)	Yes	
AU-12(b)	Partial	
AU-12(c)	Yes	
CA-1(a)	Yes	
CA-1(b)	Yes	
CA-1(c)	Yes	
CA-2(a)	Yes	
CA-2(b)	Yes	
CA-2(c)	Yes	
CA-2(d)	Yes	
CA-2(e)	Yes	
CA-2(f)	Yes	
CA-2(1)	Yes	
CA-2(3)	Yes	
CA-3(a)	Yes	
CA-3(b)	Yes	
CA-3(c)	Yes	
CA-5(a)	Yes	
CA-5(b)	Yes	
CA-6(a)	Yes	
CA-6(b)	Yes	
CA-6(c)	Yes	
CA-6(d)	Yes	
CA-6(e)	Yes	
CA-7(a)	Yes	
CA-7(b)	Yes	
CA-7(c)	Yes	
CA-7(d)	Yes	
CA-7(e)	Yes	
CA-7(f)	Yes	
CA-7(g)	Yes	
CA-7(1)	Yes	
CA-7(4)(a)	Yes	
CA-7(4)(b)	Yes	
CA-7(4)(c)	Yes	
CA-8	Yes	
CA-8(1)	Yes	
CA-8(2)	Yes	
CA-9(a)	Yes	
CA-9(b)	Yes	
CA-9(c)	Yes	
CA-9(d)	Yes	
CM-1(a)	Yes	
CM-1(b)	Yes	
CM-1(c)	Yes	
CM-2(a)	Yes	
CM-2(b)	Yes	
CM-2(2)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
CM-2(3)	Yes	
CM-2(7)(a)	Yes	
CM-2(7)(b)	Yes	
CM-3(a)	Yes	
CM-3(b)	Yes	
CM-3(c)	Yes	
CM-3(d)	Yes	
CM-3(e)	Yes	
CM-3(f)	Yes	
CM-3(g)	Yes	
CM-3(2)	Yes	
CM-3(4)	Yes	
CM-4	Yes	
CM-4(2)	Yes	
CM-5	Yes	
CM-5(1)(a)	Yes	
CM-5(1)(b)	Yes	
CM-5(5)(a)	Yes	
CM-5(5)(b)	Yes	
CM-6(a)	Yes	
CM-6(b)	Yes	
CM-6(c)	Yes	
CM-6(d)	Yes	
CM-6(1)	Yes	
CM-7(a)	Yes	
CM-7(b)	Yes	
CM-7(1)(a)	Yes	
CM-7(1)(b)	Yes	
CM-7(2)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-7(5)(a)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-7(5)(b)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-7(5)(c)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-8(a)	Yes	
CM-8(b)	Yes	
CM-8(1)	Yes	
CM-8(3)(a)	Yes	
CM-8(3)(b)	Partial	Customers are responsible for controlling the software they import. Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-9(a)	Yes	
CM-9(b)	Yes	
CM-9(c)	Yes	
CM-9(d)	Yes	
CM-9(e)	Yes	
CM-10(a)	Yes	
CM-10(b)	Yes	
CM-10(c)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
CM-11(a)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-11(b)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-11(c)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
CM-12(a)	Yes	
CM-12(b)	Yes	
CM-12(c)	Yes	
CM-12(1)	Yes	
CP-1(a)	Yes	
CP-1(b)	Yes	
CP-1(c)	Yes	
CP-2(a)	Yes	
CP-2(b)	Yes	
CP-2(c)	Yes	
CP-2(d)	Yes	
CP-2(e)	Yes	
CP-2(f)	Yes	
CP-2(g)	Yes	
CP-2(h)	Yes	
CP-2(1)	Yes	
CP-2(3)	Yes	
CP-2(8)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-3(a)	Yes	
CP-3(b)	Yes	
CP-4(a)	Yes	
CP-4(b)	Yes	
CP-4(c)	Yes	
CP-4(1)	Yes	
CP-6(a)	Yes	
CP-6(b)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-6(1)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-6(3)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-7(a)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-7(b)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-7(c)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-7(1)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
CP-7(2)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-7(3)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-8	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-8(1)(a)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-8(1)(b)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-8(2)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-9(a)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the availability of the customer's data sources.
CP-9(b)	Yes	
CP-9(c)	Yes	
CP-9(d)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the backup of the customer's data sources.
CP-9(1)	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the testing backups of the customer's data sources.
CP-9(8)	Yes	
CP-10	Partial	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks (https://docs.databricks.com/administration-guide/disaster-recovery.html) including the backup of the customer's data sources.
CP-10(2)	Yes	
IA-1(a)	Yes	
IA-1(b)	Yes	
IA-1(c)	Yes	
IA-2	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
IA-2(1)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) and ensuring their access to Databricks require multifactor authentication.
IA-2(2)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) and ensuring their access to Databricks require multifactor authentication.
IA-2(5)	Partial	Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
IA-2(6)(a)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) and ensuring their access to Databricks require multifactor authentication.
IA-2(6)(b)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) and ensuring their access to Databricks require multifactor authentication.
IA-2(8)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) and ensuring their access to Databricks require multifactor authentication.
IA-2(12)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) using an identity provider which accepts and verifies PIV credentials (e.g., Okta).
IA-3	Yes	
IA-4(a)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
IA-5(h)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(i)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(1)(a)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(1)(b)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(1)(c)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(1)(d)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(1)(e)	Partial	
IA-5(1)(f)	Yes	
IA-5(1)(g)	Yes	
IA-5(1)(h)	Yes	
IA-5(2)(a)	Yes	
IA-5(2)(b)	Yes	
IA-5(6)	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html). Customers are responsible for verifying the identity of their users.
IA-5(7)	Partial	
IA-6	Partial	Customers are responsible for configuring and provisioning access to their environment.
IA-7	Partial	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) and ensuring their access to Databricks meets applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance on cryptographic module authentication. Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html). Customers are responsible for managing user access to Databricks and administering permissions (https://docs.databricks.com/administration-guide/users-groups/groups.html).
IA-8	No	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
IA-8(1)	No	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) using an identity provider which accepts and verifies PIV credentials (e.g., Okta).
IA-8(2)(a)	No	groups/single-sign-on/index.html) using an identity provider which accepts and verifies FICAM-approved third-party credentials (e.g., Okta).
IA-8(2)(b)	No	groups/single-sign-on/index.html) using an identity provider which accepts and verifies FICAM-approved third-party credentials (e.g., Okta).
IA-8(4)	No	groups/single-sign-on/index.html) using an identity provider which accepts and verifies FICAM-approved third-party credentials (e.g., Okta).
IA-11	Yes	
IA-12(a)	Yes	
IA-12(b)	Yes	
IA-12(c)	Yes	
IA-12(2)	Yes	
IA-12(3)	Yes	
IA-12(5)	Yes	
IR-1(a)	Yes	
IR-1(b)	Yes	
IR-1(c)	Yes	
IR-2(a)	Yes	
IR-2(b)	Yes	
IR-3	Yes	
IR-3(2)	Yes	
IR-4(a)	Yes	
IR-4(b)	Yes	
IR-4(c)	Yes	
IR-4(d)	Yes	
IR-4(1)	Yes	
IR-5	Yes	
IR-6(a)	Yes	
IR-6(b)	Partial	Customers are responsible reporting incidents to Databricks.
IR-6(1)	Yes	
IR-6(3)	Yes	
IR-7	Yes	
IR-7(1)	Yes	
IR-8(a)	Yes	
IR-8(b)	Yes	
IR-8(c)	Yes	
IR-8(d)	Yes	
IR-8(e)	Yes	
IR-9(a)	Yes	
IR-9(b)	Yes	
IR-9(c)	Yes	
IR-9(d)	Yes	
IR-9(e)	Yes	
IR-9(f)	Yes	
IR-9(g)	Yes	
IR-9(2)	Yes	
IR-9(3)	Yes	
IR-9(4)	Yes	
MA-1(a)	Yes	
MA-1(b)	Yes	
MA-1(c)	Yes	
MA-2(a)	Yes	
MA-2(b)	Yes	
MA-2(c)	Yes	
MA-2(d)	Yes	
MA-2(e)	Yes	
MA-2(f)	Yes	
MA-3(a)	Yes	
MA-3(b)	Yes	
MA-3(1)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
MA-3(2)	Yes	
MA-3(3)(a)	Yes	
MA-3(3)(b)	Yes	
MA-3(3)(c)	Yes	
MA-3(3)(d)	Yes	
MA-4(a)	Yes	
MA-4(b)	Yes	
MA-4(c)	Yes	
MA-4(d)	Yes	
MA-4(e)	Yes	
MA-5(a)	Yes	
MA-5(b)	Yes	
MA-5(c)	Yes	
MA-5(1)(a)	Yes	
MA-5(1)(b)	Yes	
MA-6	Yes	
MP-1(a)	Yes	
MP-1(b)	Yes	
MP-1(c)	Yes	
MP-2	Yes	
MP-3(a)	Yes	
MP-3(b)	Yes	
MP-4(a)	Yes	
MP-4(b)	Yes	
MP-5(a)	Yes	
MP-5(b)	Yes	
MP-5(c)	Yes	
MP-5(d)	Yes	
MP-6(a)	Yes	
MP-6(b)	Yes	
MP-7(a)	Yes	
MP-7(b)	Yes	
PE-1(a)	Yes	
PE-1(b)	Yes	
PE-1(c)	Yes	
PE-2(a)	Yes	
PE-2(b)	Yes	
PE-2(c)	Yes	
PE-2(d)	Yes	
PE-3(a)	Yes	
PE-3(b)	Yes	
PE-3(c)	Yes	
PE-3(d)	Yes	
PE-3(e)	Yes	
PE-3(f)	Yes	
PE-3(g)	Yes	
PE-4	Yes	
PE-5	Yes	
PE-6(a)	Yes	
PE-6(b)	Yes	
PE-6(c)	Yes	
PE-6(1)	Yes	
PE-8(a)	Yes	
PE-8(b)	Yes	
PE-8(c)	Yes	
PE-9	Yes	
PE-10(a)	Yes	
PE-10(b)	Yes	
PE-10(c)	Yes	
PE-11	Yes	
PE-12	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
PE-13	Yes	
PE-13(1)	Yes	
PE-13(2)(a)	Yes	
PE-13(2)(b)	Yes	
PE-14(a)	Yes	
PE-14(b)	Yes	
PE-15	Yes	
PE-16(a)	Yes	
PE-16(b)	Yes	
PE-17(a)	Yes	
PE-17(b)	Yes	
PE-17(c)	Yes	
PE-17(d)	Yes	
PL-1(a)	Yes	
PL-1(b)	Yes	
PL-1(c)	Yes	
PL-2(a)	Yes	
PL-2(b)	Yes	
PL-2(c)	Yes	
PL-2(d)	Yes	
PL-2(e)	Yes	
PL-4(a)	Yes	
PL-4(b)	Yes	
PL-4(c)	Yes	
PL-4(d)	Yes	
PL-4(1)(a)	Yes	
PL-4(1)(b)	Yes	
PL-4(1)(c)	Yes	
PL-8(a)	Yes	
PL-8(b)	Yes	
PL-8(c)	Yes	
PL-10	Yes	
PL-11	Yes	
PS-1(a)	Yes	
PS-1(b)	Yes	
PS-1(c)	Yes	
PS-2(a)	Yes	
PS-2(b)	Yes	
PS-2(c)	Yes	
PS-3(a)	Yes	
PS-3(b)	Yes	
PS-3(3)(a)	Yes	
PS-3(3)(b)	Yes	
PS-4(a)	Yes	
PS-4(b)	Yes	
PS-4(c)	Yes	
PS-4(d)	Yes	
PS-4(e)	Yes	
PS-5(a)	Yes	
PS-5(b)	Yes	
PS-5(c)	Yes	
PS-5(d)	Yes	
PS-6(a)	Yes	
PS-6(b)	Yes	
PS-6(c)	Yes	
PS-7(a)	Yes	
PS-7(b)	Yes	
PS-7(c)	Yes	
PS-7(d)	Yes	
PS-7(e)	Yes	
PS-8(a)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
PS-8(b)	Yes	
PS-9	Yes	
RA-1(a)	Yes	
RA-1(b)	Yes	
RA-1(c)	Yes	
RA-2(a)	Yes	
RA-2(b)	Yes	
RA-2(c)	Yes	
RA-3(a)	Yes	
RA-3(b)	Yes	
RA-3(c)	Yes	
RA-3(d)	Yes	
RA-3(e)	Yes	
RA-3(f)	Yes	
RA-3(1)(a)	Yes	
RA-3(1)(b)	Yes	
RA-5(a)	Yes	
RA-5(b)	Yes	
RA-5(c)	Yes	
RA-5(d)	Yes	
RA-5(e)	Yes	
RA-5(f)	Yes	
RA-5(2)	Yes	
RA-5(3)	Yes	
RA-5(5)	Yes	
RA-5(11)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and monitoring these logs.
RA-7	Yes	
RA-9	Yes	
SA-1(a)	Yes	
SA-1(b)	Yes	
SA-1(c)	Yes	
SA-2(a)	Yes	
SA-2(b)	Yes	
SA-2(c)	Yes	
SA-3(a)	Yes	
SA-3(b)	Yes	
SA-3(c)	Yes	
SA-3(d)	Yes	
SA-4(a)	Yes	
SA-4(b)	Yes	
SA-4(c)	Yes	
SA-4(d)	Yes	
SA-4(e)	Yes	
SA-4(f)	Yes	
SA-4(g)	Yes	
SA-4(h)	Yes	
SA-4(i)	Yes	
SA-4(1)	Yes	
SA-4(2)	Yes	
SA-4(9)	Yes	
SA-4(10)	No	Customers are responsible for setting up single sign-on (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html) using an identity provider which accepts and verifies PIV credentials (e.g., Okta).
SA-5(a)	Yes	
SA-5(b)	Yes	
SA-5(c)	Yes	
SA-5(d)	Yes	
SA-8	Yes	
SA-9(a)	Yes	
SA-9(b)	Yes	
SA-9(c)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
SA-9(1)(a)	Yes	
SA-9(1)(b)	Yes	
SA-9(2)	Yes	
SA-9(5)	Yes	
SA-10(a)	Yes	
SA-10(b)	Yes	
SA-10(c)	Yes	
SA-10(d)	Yes	
SA-10(e)	Yes	
SA-11(a)	Yes	
SA-11(b)	Yes	
SA-11(c)	Yes	
SA-11(d)	Yes	
SA-11(e)	Yes	
SA-11(1)	Yes	
SA-11(2)(a)	Yes	
SA-11(2)(b)	Yes	
SA-11(2)(c)	Yes	
SA-11(2)(d)	Yes	
SA-15(a)	Yes	
SA-15(b)	Yes	
SA-15(3)(a)	Yes	
SA-15(3)(b)	Yes	
SA-22(a)	Yes	
SA-22(b)	Yes	
SC-1(a)	Yes	
SC-1(b)	Yes	
SC-1(c)	Yes	
SC-2	Yes	
SC-4	Yes	
SC-5(a)	Yes	
SC-5(b)	Yes	
SC-7(a)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SC-7(b)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SC-7(c)	Partial	Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SC-7(3)	Partial	Customers are responsible for managing the networking of their AWS account. Customers are responsible for controlling the software they import. Customers are responsible for managing connections to/from their Databricks workspace including, but not limited to the following: <ul style="list-style-type: none"> IP access lists to further restrict access to their Databricks instance (https://docs.databricks.com/security/network/ip-access-list.html). Mounting their data sources (https://docs.databricks.com/data/data-sources/index.html).
SC-7(4)(a)	Yes	
SC-7(4)(b)	Yes	
SC-7(4)(c)	Yes	
SC-7(4)(d)	Yes	
SC-7(4)(e)	Yes	
SC-7(4)(f)	Yes	
SC-7(4)(g)	Yes	
SC-7(4)(h)	Yes	
SC-7(5)	Yes	
SC-7(7)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
SC-7(8)	Yes	
SC-7(12)	Partial	The customer is responsible for protecting their data from exfiltration, such as mechanisms described in the following link: https://www.databricks.com/blog/2021/02/02/data-exfiltration-protection-with-databricks-on-aws.html .
SC-7(18)	Yes	
SC-8	Yes	
SC-8(1)	Yes	
SC-10	Partial	Customers are responsible for initiating a session timeout within their identity provider.
SC-12	Yes	
SC-13(a)	Partial	Customers are responsible for configuring and supporting their cryptographic keys. Customers are responsible for allowing Databricks to GetBucketLocation to ensure Databricks uses the FIPS AWS S3 endpoint for Audit Log Delivery.
SC-13(b)	Partial	
SC-15(a)	Yes	
SC-15(b)	Yes	
SC-17(a)	Yes	
SC-17(b)	Yes	
SC-18(a)	Yes	
SC-18(b)	Yes	
SC-20(a)	Yes	
SC-20(b)	Yes	
		Customers are responsible for using Customer-managed VPC (https://docs.databricks.com/administration-guide/cloud-configurations/aws/customer-managed-vpc.html) and ensuring the Databricks data plane components request and perform data origin authentication and data integrity verification on the name/address resolution responses for the system receives from authoritative sources.
SC-21	Partial	
SC-22	Yes	
SC-23	Yes	
SC-28	Yes	
		Customers are responsible for protecting the confidentiality and integrity of their data sources, such as Google BigQuery, MongoDB, Amazon Redshift, CSV files, images, JSON files, MLflow experiments, Parquet files, XML files, and Zip files. (https://docs.databricks.com/data/data-sources/index.html)
SC-28(1)	Partial	Customers are responsible for configuring Databricks Customer Managed Keys (CMK).
SC-39	Yes	
SC-45	Yes	
SC-45(1)(a)	Yes	
SC-45(1)(b)	Yes	
SI-1(a)	Yes	
SI-1(b)	Yes	
SI-1(c)	Yes	
SI-2(a)	Yes	
SI-2(b)	Yes	
SI-2(c)	Yes	
SI-2(d)	Yes	
SI-2(2)	Yes	
SI-2(3)(a)	Yes	
SI-2(3)(b)	Yes	
SI-3(a)	Yes	
SI-3(b)	Yes	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and reviewing the anti-virus alerts. Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
SI-3(c)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and reviewing the anti-virus alerts. Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
SI-3(d)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery) and reviewing the anti-virus alerts. Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.
SI-4(a)	Partial	
SI-4(b)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-4(c)	Partial	
SI-4(d)	Yes	
SI-4(e)	Yes	
SI-4(f)	Yes	
SI-4(g)	Yes	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-4(1)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-4(2)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-4(4)(a)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-4(4)(b)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-4(5)	Partial	
SI-4(16)	Yes	
		The customer is responsible for protecting their data from exfiltration, such as mechanisms described in the following link: https://www.databricks.com/blog/2021/02/02/data-exfiltration-protection-with-databricks-on-aws.html .
SI-4(18)	Partial	
SI-4(23)	Yes	
SI-5(a)	Yes	
SI-5(b)	Yes	
SI-5(c)	Yes	
SI-5(d)	Yes	
SI-6(a)	Yes	
SI-6(b)	Yes	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-6(c)	Partial	
		Customers are responsible configuring Databricks Audit Log Delivery (https://docs.databricks.com/administration-guide/account-settings/audit-logs.html#configure-audit-log-delivery). Customers are responsible for ingesting and responding to events delivered to the customer's S3 bucket.
SI-6(d)	Partial	
SI-7(a)	Yes	
SI-7(b)	Yes	
SI-7(1)	Yes	
SI-7(7)	Yes	
SI-8(a)	Yes	
SI-8(b)	Yes	
SI-8(2)	Yes	
SI-10	Yes	
SI-11(a)	Yes	
SI-11(b)	Yes	
SI-12	Yes	
SI-16	Yes	
SR-1(a)	Yes	
SR-1(b)	Yes	
SR-1(c)	Yes	
SR-2(a)	Yes	

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
SR-2(b)	Yes	
SR-2(c)	Yes	
SR-2(1)	Yes	
SR-3(a)	Yes	
SR-3(b)	Yes	
SR-3(c)	Yes	
SR-5	Yes	
SR-6	Yes	
SR-8	Yes	
SR-10	Yes	
SR-11(a)	Yes	
SR-11(b)	Yes	
SR-11(1)	Yes	
SR-11(2)	Yes	
SR-12	Yes	