NIST SP 800-53 Rev5
Written Information Security Program (WISP) Mapping Matrix

NIST 800-53 R5 # Low / Mod / High	NIST SP 800-53 R5 Control Name	CSOP Procedures #	Tailoring Guidance		NIST SP 800-53 R5 Baseline					FedRAMP Baseline				CMMC v1.02					Common Statutory, Regulatory & Contractual Frameworks That Map To NIST SP 800-53 R5																					
			Target Audience	Applicability	Privacy	Low	Moderate	High	NOC	Low	Moderate	High	LI-SaaS	Level 1	Level 2	Level 3	Level 4	Level 5	AICPA TSC 2017	CERT RMM	CIS CSC v7.1	FACTA	FAR 52.204-21	Generally Accepted	GLBA	HIPAA	ISO 27002	IRS 1075	MA 201 CMR	NERC CIP	NISPOM	NIST CSF v1.1	NIST 800-171 rev 2	NIST 800-171A	NIST 800-172 [draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2.1	Secure Controls	UK Cyber
AC-1	**Policy and Procedures**	**P-AC-1**	Management	Basic	x	x	x	x		AC-1	AC-1	AC-1	AC-1						CC5.1 CC5.2	AM:SG1.SP1	4.4 16.1			8.2.2		164.308(a)(3)(i) 164.308(a)(3)(ii)(A	5.1.1 5.1.2	9.3.1.1			8-101 8-606							8.1 8.4	IAC-01	
AC-2	**Account Management**	**P-AC-2**	Management	Basic		x	x	x		AC-2	AC-2	AC-2	AC-2	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	CC6.2 CC7.2	AM:SG1.SP1 AM:SG1.SP2	4.4 16.1			8.2.2		164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(A	9.2.1 9.2.2	9.3.1.2	17.04(1(a)		8-606	PR.AC-1 PR.AC-4	3.1.1 3.1.2	3.1.1[a] 3.1.1[b]				8.1.3 8.1.4	IAC-07.2 IAC-15	
AC-2(1)	automated system account management	P-AC-2(1)	Technical Users	Enhanced			x	x			AC-2(1)	AC-2(1)							CC6.2		16.2																		IAC-15.1	
AC-2(2)	automated temporary and emergency account management	P-AC-2(2)	Technical Users	Enhanced			x	x			AC-2(2)	AC-2(2)							CC6.2		16.8																		IAC-15.2	2-1
AC-2(3)	disable accounts	P-AC-2(3)	Technical Users	Enhanced			x	x			AC-2(3)	AC-2(3)							CC6.2		16.8													3.5.6[a] 3.5.6[b]					IAC-15.3	2-1 3-7
AC-2(4)	automated audit actions	P-AC-2(4)	Technical Users	Enhanced			x	x			AC-2(4)	AC-2(4)							CC6.2		16.9																		IAC-15.4	
AC-2(5)	inactivity logout	P-AC-2(5)	Technical Users	Basic			x	x			AC-2(5)	AC-2(5)							CC6.1		16.11																		IAC-24	
AC-2(6)	dynamic privilege management	N/A	N/A	N/A					x																															
AC-2(7)	privileged user accounts	P-AC-2(7)	Management	Basic					x		AC-2(7)	AC-2(7)							CC6.3		14.6																	7.1 7.1.1	IAC-08	3-1
AC-2(8)	dynamic account management	N/A	N/A	N/A					x																															
AC-2(9)	restrictions on use of shared and group accounts	P-AC-2(9)	Technical Users	Basic					x		AC-2(9)	AC-2(9)							CC6.2																				IAC-15.5	
AC-2(10)	shared and group account credential change [Incorporated into AC-2k]	N/A	N/A	N/A							AC-2(10)	AC-2(10)							CC6.2		16.7																		IAC-07.2	
AC-2(11)	usage conditions	P-AC-2(11)	Technical Users	Enhanced				x				AC-2(11)							CC6.1																				IAC-15.8	
AC-2(12)	account monitoring for atypical usage	P-AC-2(12)	Technical Users	Enhanced				x			AC-2(12)	AC-2(12)							CC7.2		16.8 16.13																		MON-16	
AC-2(13)	disable accounts for high-risk individuals	P-AC-2(13)	Technical Users	Enhanced			x	x				AC-2(13)							CC7.3 CC7.4																				IAC-15.6	
AC-3	**Access Enforcement**	**P-AC-3**	Management	Basic		x	x	x		AC-3	AC-3	AC-3	AC-3	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	CC6.1	AM:SG1.SP1 TM:SG4.SP1						164.308(a)(3)(ii)(A)	6.2.2 9.1.2	9.3.1.3	17.04(1)(b) 17.04(2)(a)		8-606	PR.AM-3 PR.AC-4	3.1.1 3.1.2	3.1.2[a] 3.1.2[b]	3.14.3e		622(2)(d)(C)(iii)	7.1 7.1.1	IAC-20	
AC-3(1)	restricted access to privileged function [Incorporated into AC-6]	N/A	N/A	N/A																																				
AC-3(2)	dual authorization	P-AC-3(2)	Technical Users	Enhanced					x										CC6.1																3.1.1e				HRS-12.1 IAC-20.5	
AC-3(3)	mandatory access control	N/A	N/A	N/A					x																															
AC-3(4)	discretionary access control	N/A	N/A	N/A					x																															
AC-3(5)	security-relevant information	N/A	N/A	N/A					x																															
AC-3(6)	protection of user and system information [Incorporated into MP-4, SC-28]	N/A	N/A	N/A																																				
AC-3(7)	role-based access control	N/A	N/A	N/A					x																															
AC-3(8)	revocation of access authorizations	N/A	N/A	N/A					x																															
AC-3(9)	controlled release	N/A	N/A	N/A					x																															
AC-3(10)	audited override of access control mechanisms	N/A	N/A	N/A					x																															
AC-3(11)	restrict access to specific information types	N/A	N/A	N/A					x																															
AC-3(12)	assert and enforce application access	N/A	N/A	N/A					x																															
AC-3(13)	attribute-based access control	N/A	N/A	N/A					x																															
AC-3(14)	individual access	P-AC-3(14)	Technical Users	Basic	x				x																															
AC-3(15)	discretionary and mandatory access control	N/A	N/A	N/A					x																															
AC-4	**Information Flow Enforcement**	**P-AC-4**	Technical Users	Basic			x	x			AC-4	AC-4			AC.2.016	AC.2.016	AC.2.016 AC.4.023	AC.2.016 AC.4.023	CC6.1	TM:SG4.SP1	[illegible]					164.308(a)(3)(ii)(A	8.2.2 8.2.3	9.3.1.4				PR.AC-5 PR.DS-5	3.1.3	3.1.3[a] 3.1.3[b]	3.1.3e 3.11.4e		622(2)(d)(C)(iii)	1.1.6 1.3.3	NET-04	
AC-4(1)	object security and privacy attributes	P-AC-4(1)	Technical Users	Basic					x								AC.4.023	AC.4.023																	3.1.3e				NET-04.2	
AC-4(2)	processing domains	N/A	N/A	N/A					x																															
AC-4(3)	dynamic information flow control	N/A	N/A	N/A					x																															
AC-4(4)	flow control of encrypted information	P-AC-4(4)	Technical Users	Enhanced				x													[illegible]																		NET-04.3	
AC-4(5)	embedded data types	N/A	N/A	N/A					x												[illegible]																		NET-04.4	
AC-4(6)	metadata	P-AC-4(6)	Technical Users	Enhanced					x								AC.4.023	AC.4.023																	3.1.3e				NET-04.5	
AC-4(7)	one-way flow mechanisms	N/A	N/A	N/A					x																															
AC-4(8)	security and privacy policy filters	P-AC-4(8)	Technical Users	Enhanced					x			AC-4(8)				SC.3.192	SC.3.192 AC.4.023	SC.3.192 AC.4.023																	3.1.3e				NET-04.7	
AC-4(9)	human reviews	N/A	N/A	N/A					x																													1.1.7	NET-04.6	1-4
AC-4(10)	enable and disable security or privacy policy filters	N/A	N/A	N/A					x																															
AC-4(11)	configuration of security or privacy policy filters	N/A	N/A	N/A					x																															
AC-4(12)	data type identifiers	P-AC-4(12)	Technical Users	Enhanced					x								AC.4.023	AC.4.023																	3.1.3e				NET-04.8	
AC-4(13)	decomposition into policy-relevant subcomponents	P-AC-4(13)	Technical Users	Enhanced					x								AC.4.023	AC.4.023																	3.1.3e				NET-04.9	
AC-4(14)	security or privacy policy filter constraints	N/A	N/A	N/A					x																															
AC-4(15)	detection of unsanctioned information	P-AC-4(15)	Technical Users	Enhanced					x								AC.4.023	AC.4.023																	3.1.3e				NET-04.10	
AC-4(16)	information transfers on interconnected systems [Incorporated into AC-4]	N/A	N/A	N/A																																				
AC-4(17)	domain authentication	N/A	N/A	N/A					x																															
AC-4(18)	security attribute binding [Incorporated into AC-16]	N/A	N/A	N/A																																				
AC-4(19)	validation of metadata	N/A	N/A	N/A					x																															
AC-4(20)	approved solutions	P-AC-4(20)	Technical Users	Enhanced					x								AC.4.023	AC.4.023																	3.1.3e				NET-04.11	
AC-4(21)	physical or logical separation of information flows	P-AC-4(21)	Technical Users	Enhanced					x		AC-4(21)	AC-4(21)									11.7 14.1																		NET-06	
AC-4(22)	access only	N/A	N/A	N/A					x																															
AC-4(23)	modify non-releasable information	N/A	N/A	N/A					x																															
AC-4(24)	internal normalized format	N/A	N/A	N/A					x																															
AC-4(25)	data sanitization	N/A	N/A	N/A					x																															
AC-4(26)	audit filtering actions	N/A	N/A	N/A					x																															
AC-4(27)	redundant/independent filtering mechanisms	N/A	N/A	N/A					x																															
AC-4(28)	linear filter pipelines	N/A	N/A	N/A					x																															
AC-4(29)	filter orchestration engines	N/A	N/A	N/A					x																															
AC-4(30)	filter mechanisms using multiple processes	N/A	N/A	N/A					x																															
AC-4(31)	failed content transfer prevention	N/A	N/A	N/A					x																															
AC-4(32)	process requirements for information transfer	N/A	N/A	N/A					x																															
AC-5	**Separation of Duties**	**P-AC-5**	Management	Enhanced			x	x			AC-5	AC-5				AC.3.017	AC.3.017	AC.3.017	CC6.1	AM:SG1.SP1 ID:SG1.SP1						164.308(a)(3)(i) 164.308(a)(4)(i)	6.1.2	9.3.1.5			8-611	PR.AC-4 PR.DS-5	3.1.4	3.1.4[a] 3.1.4[b]				6.4.2	CHG-04.3 HRS-11	
AC-6	**Least Privilege**	**P-AC-6**	Management	Basic			x	x			AC-6	AC-6			AC.2.007	AC.2.007	AC.2.007	AC.2.007		AM:SG1.SP1 ID:SG1.SP1	14.6					164.308(a)(3)(i) 164.308(a)(4)(i)	9.1.2 9.2.3	9.3.1.6			8-303	PR.AC-4 PR.DS-5	3.1.5	3.1.5[a] 3.1.5[b]			622(2)(d)(C)(iii)		IAC-21	3-2 3-7
AC-6(1)	authorize access to security functions	P-AC-6(1)	Technical Users	Basic			x	x			AC-6(1)	AC-6(1)			AC.2.007	AC.2.007	AC.2.007	AC.2.007	CC6.3														3.1.5						IAC-21.1	
AC-6(2)	non-privileged access for nonsecurity functions	P-AC-6(2)	Technical Users	Basic			x	x			AC-6(2)	AC-6(2)			AC.2.008	AC.2.008	AC.2.008	AC.2.008															3.1.6	3.1.6[a] 3.1.6[b]				10.2 10.2.1	IAC-21.2	3-2
AC-6(3)	network access to privileged commands	P-AC-6(3)	Technical Users	Enhanced				x				AC-6(3)																											IAC-21.6	
AC-6(4)	separate processing domains	N/A	N/A	N/A					x																															
AC-6(5)	privileged accounts	P-AC-6(5)	Technical Users	Basic			x	x			AC-6(5)	AC-6(5)			AC.2.007	AC.2.007	AC.2.007	AC.2.007	CC6.3														3.1.5						IAC-21.3	3-2 3-3
AC-6(6)	privileged access by non-organizational users	N/A	N/A	N/A					x																															
AC-6(7)	review of user privileges	P-AC-6(7)	Management	Basic			x	x				AC-6(7)					AC.4.025	AC.4.025	CC6.3		4.3 16.13																		IAC-17	
AC-6(8)	privilege levels for code execution	P-AC-6(8)	Technical Users	Enhanced					x			AC-6(8)							CC6.3																				IAC-21.7	
AC-6(9)	log use of privileged functions	P-AC-6(9)	Technical Users	Basic			x	x			AC-6(9)	AC-6(9)				AC.3.018	AC.3.018	AC.3.018	CC7.2		4.3												3.1.7	3.1.7[d]				10.2 10.2.1	IAC-21.4	3-3
AC-6(10)	prohibit non-privileged users from executing privileged functions	P-AC-6(10)	Technical Users	Basic			x	x			AC-6(10)	AC-6(10)				AC.3.018	AC.3.018	AC.3.018	CC6.1		4.8												3.1.7						IAC-21.5	3-2 3-4
AC-7	**Unsuccessful Logon Attempts**	**P-AC-7**	Management	Basic		x	x	x		AC-7	AC-7	AC-7	AC-7		AC.2.009	AC.2.009	AC.2.009	AC.2.009	CC6.1	TM:SG4.SP1	16.11						9.4.2	9.3.1.7	17.04(1)(e)		8-609		3.1.8	3.1.8[a] 3.1.8[b]				8.1.6 8.1.7	IAC-22	
AC-7(1)	automatic account lock [Incorporated into AC-7]	N/A	N/A	N/A																																				
AC-7(2)	purge or wipe mobile device	P-AC-7(2)	Management	Basic					x			AC-7(2)							CC6.6																				MDM-05	
AC-7(3)	biometric attempt limiting	N/A	N/A	N/A					x																															

R5 # Low / Mod / High	Control Name	Procedures #	Target Audience	Applicability	Privacy	Low	Moderate	High	NOC	Low	Moderate	High	LI-SaaS	Level 1	Level 2	Level 3	Level 4	Level 5	AICPA TSC 2017	CERT RMM	CIS CSC v7.1	FACTA	FAR 52.204-21	Generally Accepted	GLBA	HIPAA	ISO 27002	IRS 1075	MA 201 CMR	NERC CIP	NISPOM	NIST CSF v1.1	NIST 800-171 rev 2	NIST 800-171A	NIST 800-172 [draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2.1	Secure Controls	UK Cyber
AC-7(4)	use of alternate authentication factor	N/A	N/A	N/A					x																															
AC-8	**System Use Notification**	**P-AC-8**	Technical Users	Basic		x	x	x		AC-8	AC-8	AC-8	AC-8		AC.2.005	AC.2.005	AC.2.005	AC.2.005		TM:SG4.SP1							9.4.2	9.3.1.8			8-609		3.1.9	3.1.9[a] 3.1.9[b]					SEA-18	
AC-9	**Previous Logon Notification**	N/A	N/A	N/A					x										CC6.1	TM:SG4.SP1							9.4.2				8-609								SEA-19	
AC-9(1)	unsuccessful logons	N/A	N/A	N/A					x																															
AC-9(2)	successful and unsuccessful logons	N/A	N/A	N/A					x																															
AC-9(3)	notification of account changes	N/A	N/A	N/A					x																															
AC-9(4)	additional logon information	N/A	N/A	N/A					x																															
AC-10	**Concurrent Session Control**	**P-AC-10**	Technical Users	Basic				x			AC-10	AC-10							CC6.1	AM:SG1.SP1											8-609								IAC-23	
AC-11	**Device Lock**	**P-AC-11**	Technical Users	Basic			x	x			AC-11	AC-11			AC.2.010	AC.2.010	AC.2.010	AC.2.010	CC6.1	TM:SG4.SP1	16.11					164.310(b) 164.312(a)(2)(iii)	9.4.2 11.2.8	9.3.1.9			8-609		3.1.10	3.1.10[a] 3.1.10[b]					IAC-24	
AC-11(1)	pattern-hiding displays	P-AC-11(1)	Technical Users	Basic			x	x			AC-11(1)	AC-11(1)			AC.2.010	AC.2.010	AC.2.010	AC.2.010	CC6.1														3.1.10						IAC-24.1	
AC-12	**Session Termination**	**P-AC-12**	Technical Users	Basic			x	x			AC-12	AC-12				AC.3.019	AC.3.019	AC.3.019	CC6.1	AM:SG1.SP1						164.310(b) 164.312(a)(2)(iii)	9.4.2	9.3.1.10			8-311 8-609		3.1.11	3.1.11[a] 3.1.11[b]				8.1.8	IAC-25	
AC-12(1)	user-initiated logouts	P-AC-12(1)	Technical Users	Enhanced					x			AC-12(1)							CC6.1																				IAC-25.1	
AC-12(2)	termination message	N/A	N/A	N/A					x																															
AC-12(3)	timeout warning message	N/A	N/A	N/A					x																															
AC-13	**Supervision and Review-Access Control [Incorporated into AC-2, AU-6]**	N/A	N/A	N/A																																				
AC-14	**Permitted Actions without Identification or Authentication**	**P-AC-14**	Technical Users	Basic		x	x	x		AC-14	AC-14	AC-14	AC-14						CC6.1	IMC:SG1.SP1 TM:SG2.SP1								9.3.1.11			8-501 8-504								IAC-26	
AC-14(1)	necessary uses [Incorporated into AC-14]	N/A	N/A	N/A																																				
AC-15	**Automated Marking [Incorporated into MP-3]**	N/A	N/A	N/A																																				
AC-16	**Security and Privacy Attributes**	N/A	N/A	N/A					x										CC6.1	KIM:SG2.SP1 KIM:SG2.SP2						164.310(b)	8.2.2 8.2.3				8-306	PR.AC-4							DCH-05	
AC-16(1)	dynamic attribute association	N/A	N/A	N/A					x																															
AC-16(2)	attribute value changes by authorized individuals	N/A	N/A	N/A					x																															
AC-16(3)	maintenance of attribute associations by system	N/A	N/A	N/A					x																															
AC-16(4)	association of attributes by authorized individuals	N/A	N/A	N/A					x																															
AC-16(5)	attribute displays on objects to be output	N/A	N/A	N/A					x																															
AC-16(6)	maintenance of attribute association	N/A	N/A	N/A					x																															
AC-16(7)	consistent attribute interpretation	N/A	N/A	N/A					x																															
AC-16(8)	association techniques and technologies	N/A	N/A	N/A					x																															
AC-16(9)	attribute reassignment – regrading mechanisms	N/A	N/A	N/A					x																															
AC-16(10)	attribute configuration by authorized individuals	N/A	N/A	N/A					x																															
AC-17	**Remote Access**	**P-AC-17**	All Users	Basic		x	x	x		AC-17	AC-17	AC-17	AC-17	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	AC.1.001 AC.1.002	CC6.6	TM:SG4.SP1	12.12					164.310(b)	6.2.1 6.2.2	9.3.1.12				PR.AC-3 PR.PT-4	3.1.1 3.1.2					8.1.5 12.3.8	NET-14	
AC-17(1)	monitoring and control	P-AC-17(1)	All Users	Enhanced			x	x			AC-17(1)	AC-17(1)			AC.2.013	AC.2.013	AC.2.013 AC.4.032	AC.2.013 AC.4.032	CC6.6														3.1.12	3.1.12[a] 3.1.12[b]					NET-14.1	
AC-17(2)	protection of confidentiality and integrity using encryption	P-AC-17(2)	All Users	Enhanced			x	x			AC-17(2)	AC-17(2)				AC.3.014	AC.3.014	AC.3.014	CC6.6														3.1.13	3.1.13[a] 3.1.13[b]		500.15			NET-14.2	
AC-17(3)	managed access control points	P-AC-17(3)	All Users	Enhanced			x	x			AC-17(3)	AC-17(3)			AC.2.015	AC.2.015	AC.2.015	AC.2.015	CC6.6														3.1.14	3.1.14[a] 3.1.14[b]					NET-14.3	1-5
AC-17(4)	privileged commands and access	P-AC-17(4)	Management	Basic			x	x			AC-17(4)	AC-17(4)				AC.3.021	AC.3.021	AC.3.021	CC6.6														3.1.15	3.1.15[a] 3.1.15[b]					NET-14.4	1-5
AC-17(5)	monitoring for unauthorized connections [Incorporated into SI-4]	N/A	N/A	N/A																																				
AC-17(6)	protection of mechanism information	N/A	N/A	N/A					x												12.12																		NET-14	
AC-17(7)	additional protection for security function access [Incorporated into AC-3(10)]	N/A	N/A	N/A																																				
AC-17(8)	disable nonsecure network protocols [Incorporated into CM-7]	N/A	N/A	N/A																																				
AC-17(9)	disconnect or disable access	P-AC-17(9)	Technical Users	Enhanced					x		AC-17(9)	AC-17(9)							CC6.6																				NET-14.8	
AC-17(10)	authenticate remote commands	N/A	N/A	N/A					x																															
AC-18	**Wireless Access**	**P-AC-18**	Management	Basic		x	x	x		AC-18	AC-18	AC-18	AC-18		AC.2.011	AC.2.011	AC.2.011	AC.2.011	CC6.6	TM:SG4.SP1							6.2.1 13.1.1	9.3.1.13			8-311	PR.PT-4	3.1.16	3.1.16[a] 3.1.16[b]					CRY-07 NET-15	
AC-18(1)	authentication and encryption	P-AC-18(1)	Technical Users	Basic			x	x			AC-18(1)	AC-18(1)				AC.3.012	AC.3.012	AC.3.012	CC6.6														3.1.17	3.1.17[a] 3.1.17[b]				4.1.1	NET-15.1	
AC-18(2)	monitoring unauthorized connections [Incorporated into SI-4]	N/A	N/A	N/A																																				
AC-18(3)	disable wireless networking	P-AC-18(3)	Technical Users	Enhanced			x	x				AC-18(3)							CC8.1		15.4 15.9																		NET-15.2	
AC-18(4)	restrict configurations by users	P-AC-18(4)	Technical Users	Enhanced				x				AC-18(4)							CC6.6		15.5 15.6																		NET-15.3	
AC-18(5)	antennas and transmission power levels	P-AC-18(5)	Technical Users	Basic				x				AC-18(5)							CC6.6																				NET-15.4	
AC-19	**Access Control for Mobile Devices**	**P-AC-19**	All Users	Basic		x	x	x		AC-19	AC-19	AC-19	AC-19			AC.3.020	AC.3.020	AC.3.020	CC6.6	TM:SG4.SP1 TM:SG4.SP2						164.310(b)	6.2.1 8.2.3	9.3.1.14			8-610	PR.AC-3	3.1.18	3.1.18[a] 3.1.18[c]					MDM-02	
AC-19(1)	use of writable and portable storage devices [Incorporated into MP-7]	N/A	N/A	N/A																																				
AC-19(2)	use of personally owned portable storage devices [Incorporated into MP-7]	N/A	N/A	N/A																																				
AC-19(3)	use of portable storage devices with no identifiable owner [Incorporated into MP-7]	N/A	N/A	N/A																																				
AC-19(4)	restrictions for classified information	N/A	N/A	N/A					x																															
AC-19(5)	full device or container-based encryption	P-AC-19(5)	All Users	Enhanced			x	x			AC-19(5)	AC-19(5)				AC.3.022	AC.3.022	AC.3.022	CC6.1														3.1.19	3.1.18[a] 3.1.19[b]		500.15			MDM-03	
AC-20	**Use of External Systems**	**P-AC-20**	All Users	Basic		x	x	x		AC-20	AC-20	AC-20	AC-20	AC.1.003	AC.1.003	AC.1.003	AC.1.003	AC.1.003		EXD:SG3.SP1							8.1.3 9.1.2	9.3.1.15			8-700	ID.AM-4 PR.AC-3	3.1.20	3.1.20[a] 3.1.20[b]					DCH-13	
AC-20(1)	limits on authorized use	P-AC-20(1)	All Users	Basic			x	x			AC-20(1)	AC-20(1)		AC.1.003	AC.1.003	AC.1.003	AC.1.003	AC.1.003	CC6.6														3.1.20						DCH-13.1	
AC-20(2)	portable storage devices — restricted use	P-AC-20(2)	All Users	Basic			x	x			AC-20(2)	AC-20(2)			AC.2.006	AC.2.006	AC.2.006	AC.2.006	CC6.6														3.1.21	3.1.21[a] 3.1.21[b]					DCH-13.2	
AC-20(3)	non-organizationally owned systems — restricted use	P-AC-20(3)	All Users	Basic					x										CC6.6																3.1.2e				DCH-13.4	
AC-20(4)	network accessible storage devices — prohibited use	N/A	N/A	N/A					x																															
AC-20(5)	portable storage devices — prohibited use	N/A	N/A	N/A					x																															
AC-21	**Information Sharing**	**P-AC-21**	Technical Users	Basic			x	x			AC-21	AC-21							CC6.3	KIM:SG2.SP1 KIM:SG2.SP2								9.3.1.16				PR.IP-8							DCH-14	
AC-21(1)	automated decision support	N/A	N/A	N/A					x																															
AC-21(2)	information search and retrieval	N/A	N/A	N/A					x										CC6.1																				DCH-14.1	
AC-22	**Publicly Accessible Content**	**P-AC-22**	Technical Users	Basic		x	x	x		AC-22	AC-22	AC-22	AC-22	AC.1.004	AC.1.004	AC.1.004	AC.1.004	AC.1.004	CC6.3	ID:SG1.SP2 KIM:SG1.SP2							14.1.2 9.4.1	9.3.1.17					3.1.22	3.1.22[a] 3.1.22[b]					DCH-15	
AC-23	**Data Mining Protection**	N/A	N/A	N/A					x										CC6.1	KIM:SG2.SP2 KIM:SG4.SP2																			DCH-16	
AC-24	**Access Control Decisions**	N/A	N/A	N/A					x										CC6.1	AM:SG1.SP1 KIM:SG2.SP2							9.4.1												IAC-28.1	
AC-24(1)	transmit access authorization information	N/A	N/A	N/A					x																															
AC-24(2)	no user or process identity	N/A	N/A	N/A					x																															
AC-25	**Reference Monitor**	N/A	N/A	N/A					x										CC6.1	AM:SG1.SP1 KIM:SG4.SP2																			IAC-27	
AT-1	**Policy and Procedures**	**P-AT-1**	Management	Basic	x	x	x	x		AT-1	AT-1	AT-1	AT-1							OPD:SG1.SP1 OTA:SG1.SP1	17.2 17.3					164.308(a)(5)(i)	5.1.1 5.1.2	9.3.2.1			8-101					500.14			SAT-01	
AT-2	**Literacy Training and Awareness**	**P-AT-2**	Management	Basic	x	x	x	x		AT-2	AT-2	AT-2	AT-2		AT.2.056 AT.2.057	AT.2.056 AT.2.057	AT.2.056 AT.2.057	AT.2.056 AT.2.057		OTA:SG2.SP1	17.3 17.9					164.308(a)(5)(i) 164.308(a)(5)(ii)(A	7.2.2 12.2.1	9.3.2.2	17.04(8) 17.03(2)(b)(1)		8-101	PR.AT-1	3.2.1 3.2.2	3.2.1[a] 3.2.1[b]	3.2.1e	500.14		12.6	SAT-02	
AT-2(1)	practical exercises	P-AT-2(1)	Management	Enhanced					x								AT.4.060	AT.4.060																	3.2.2e				SAT-02.1	
AT-2(2)	insider threat	P-AT-2(2)	Management	Enhanced		x	x	x			AT-2(2)	AT-2(2)				AT.3.058	AT.3.058	AT.3.058															3.2.3	3.2.3[a] 3.2.3[b]					THR-05	
AT-2(3)	social engineering and mining	P-AT-2(3)	All Users	Basic			x	x																											3.2.1e					
AT-2(4)	suspicious communications and anomalous system behavior	P-AT-2(4)	All Users	Basic					x																										3.2.1e					
AT-2(5)	advanced persistent threat	P-AT-2(5)	Technical Users	Basic	deleted				x																															
AT-2(6)	cyber threat environment	P-AT-2(6)	Technical Users	Basic					x																										3.2.1e					
AT-3	**Role-Based Training**	**P-AT-3**	Management	Basic	x	x	x	x		AT-3	AT-3	AT-3	AT-3		AT.2.056 AT.2.057	AT.2.056 AT.2.057	AT.2.056 AT.2.057	AT.2.056 AT.2.057		OTA:SG4.SP1	17.2 17.9					164.308(a)(5)(i)	7.2.2 12.2.1	9.3.2.3	17.04(8)		8-101 8-103	PR.AT-2 PR.AT-4	3.2.1 3.2.2	3.2.1[d] 3.2.2[a]		500.10 500.14	622(2)(d)(A)(iv	1.5 2.5	SAT-03	
AT-3(1)	environmental controls	N/A	N/A	N/A					x																															
AT-3(2)	physical security controls	N/A	N/A	N/A					x																															
AT-3(3)	practical exercises	P-AT-3(3)	Management	Enhanced					x			AT-3(3)																											SAT-03.1	
AT-3(4)	suspicious communications and anomalous system behavior	N/A	N/A	N/A					x			AT-3(4)																											SAT-03.6	
AT-3(5)	processing personally identifiable information	P-AT-3(5)	All Users	Basic	x				x																															

R5 # Low / Mod / High	Control Name	Procedures #	Target Audience	Applicability	Privacy	Low	Moderate	High	NOC	Low	Moderate	High	LI-SaaS	Level 1	Level 2	Level 3	Level 4	Level 5	AICPA TSC 2017	CERT RMM	CIS CSC v7.1	FACTA	FAR 52.204-21	Generally Accepted	GLBA	HIPAA	ISO 27002	IRS 1075	MA 201 CMR	NERC CIP	NISPOM	NIST CSF v1.1	NIST 800-171 rev 2	NIST 800-171A	NIST 800-172 [draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2.1	Secure Controls	UK Cyber
AT-4	**Training Records**	**P-AT-4**	Management	Basic	x	x	x	x		AT-4	AT-4	AT-4	AT-4							OTA:SG2.SP2 OTA:SG4.SP2						164.308(a)(5)(i)		9.3.2.4			8-103 8-104					500.14		12.6.2	SAT-04	
AT-5	**Contacts with Security Groups and Associations**	N/A	N/A	N/A					x												19.5																	6.2 12.4		
AT-6	**Training Feedback**	N/A	N/A	N/A					x																															
AU-1	**Policy and Procedures**	**P-AU-1**	Management	Basic	x	x	x	x		AU-1	AU-1	AU-1	AU-1						CC5.1 CC5.2	COMP:SG1.SP2 COMP:SG2.SP3	6.2 6.8					164.312(b)	5.1.1 5.1.2	9.3.3.1			8-602	PR.PT-1				500.06		10.1 10.8	MON-01	
AU-2	**Event Logging**	**P-AU-2**	Management	Basic	x	x	x	x		AU-2	AU-2	AU-2	AU-2		AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	CC7.2	COMP:SG2.SP1	6.2 6.4					164.308(a)(5)(ii)(C) 164.312(b)	9.4.4 12.4.1	9.3.3.2	17.04(4)		8-602	PR.PT-1	3.3.1 3.3.2	3.3.1[c] 3.3.1[d]		500.06	622(2)(d)(B)(iii)	10.2 10.2.1	MON-01.8 MON-02	
AU-2(1)	compilation of audit records from multiple sources [Incorporated into AU-12]	N/A	N/A	N/A																																				
AU-2(2)	selection of audit events by component [Incorporated into AU-12]	N/A	N/A	N/A																																				
AU-2(3)	reviews and updates [Incorporated into AU-2]	N/A	N/A	N/A							AU-2(3)	AU-2(3)				AU.3.045	AU.3.045	AU.3.045	CC7.2		6.2 6.4												3.3.3			500.06		10.2 10.2.1	MON-01.8 MON-02	
AU-2(4)	privileged functions [Incorporated into AC-6(9)]	N/A	N/A	N/A																																				
AU-3	**Content of Audit Records**	**P-AU-3**	Technical Users	Enhanced		x	x	x		AU-3	AU-3	AU-3	AU-3		AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	CC7.2	COMP:SG1.SP3 COMP:SG3.SP1	6.3					164.312(b)	12.4.1 12.4.3	9.3.3.3			8-602	PR.PT-1	3.3.1 3.3.2	3.3.1[a] 3.3.1[b]		500.06		10.3 10.3.1	MON-03	
AU-3(1)	additional audit information	P-AU-3(1)	Technical Users	Basic			x	x			AU-3(1)	AU-3(1)			AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	CC7.2		6.8												3.3.1 3.3.2						MON-03.1	
AU-3(2)	centralized management of planned audit record content	N/A	N/A	N/A								AU-3(2)							CC7.2																				MON-03.6	
AU-3(3)	limit personally identifiable information elements	P-AU-3(3)	Management	Basic	x				x																															
AU-4	**Audit Log Storage Capacity**	**P-AU-4**	Technical Users	Basic		x	x	x		AU-4	AU-4	AU-4	AU-4						CC7.2	TM:SG5.SP3	6.4					164.312(b)	12.1.3 12.4.2	9.3.3.4			8-602	PR.DS-4 PR.PT-1							MON-04	
AU-4(1)	transfer to alternate storage	N/A	N/A	N/A					x										CC7.2																				MON-08.1	
AU-5	**Response to Audit Logging Process Failures**	**P-AU-5**	Technical Users	Basic		x	x	x		AU-5	AU-5	AU-5	AU-5			AU.3.046	AU.3.046	AU.3.046 AU.5.055	CC7.2	COMP:SG1.SP3 TM:SG5.SP2							12.1.3 12.4.2	9.3.3.5			8-602	PR.PT-1	3.3.4	3.3.4[a] 3.3.4[b]					MON-05	
AU-5(1)	storage capacity warning	P-AU-5(1)	Technical Users	Enhanced				x				AU-5(1)							CC7.2		6.4																		MON-05.2	
AU-5(2)	real-time alerts	P-AU-5(2)	Technical Users	Enhanced				x				AU-5(2)							CC7.2																				MON-05.1	
AU-5(3)	configurable traffic volume thresholds	N/A	N/A	N/A					x																															
AU-5(4)	shutdown on failure	N/A	N/A	N/A					x																															
AU-5(5)	alternate audit logging capability	N/A	N/A	N/A					x										CC7.2	CTRL:SG2.SP1 TM:SG5.SP1											8-602	PR.PT-1							MON-13	
AU-6	**Audit Record Review, Analysis, and Reporting**	**P-AU-6**	Technical Users	Basic		x	x	x		AU-6	AU-6	AU-6	AU-6		AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	CC7.2	COMP:SG3.SP1	6.2 6.4					164.308(a)(1)(ii)(D)	12.4.1 16.1.2	9.3.3.6			8-602	PR.PT-1 DE.AE-2	3.3.1 3.3.2	3.3.3[a] 3.3.3[b]					MON-02 MON-02.6	
AU-6(1)	automated process integration	P-AU-6(1)	Technical Users	Enhanced			x	x			AU-6(1)	AU-6(1)							CC7.2		6.8																		MON-03.1	
AU-6(2)	automated security alerts [Incorporated into SI-4]	N/A	N/A	N/A																																				
AU-6(3)	correlate audit record repositories	P-AU-6(3)	Technical Users	Enhanced			x	x			AU-6(3)	AU-6(3)				AU.3.051	AU.3.051	AU.3.051	CC7.2		6.7 6.8												3.3.5	3.3.5[a] 3.3.5[b]					MON-02.1	
AU-6(4)	central review and analysis	P-AU-6(4)	Technical Users	Enhanced					x			AU-6(4)			AU.2.044	AU.2.044	AU.2.044	AU.2.044	CC7.2																				MON-02.2	
AU-6(5)	integrated analysis of audit records	P-AU-6(5)	Technical Users	Enhanced				x				AU-6(5)							CC7.2																				MON-02.3	
AU-6(6)	correlation with physical monitoring	P-AU-6(6)	Technical Users	Enhanced				x				AU-6(6)							CC7.2																3.14.2e				MON-02.4	
AU-6(7)	permitted actions	P-AU-6(7)	Technical Users	Enhanced					x			AU-6(7)							CC7.3 CC7.4																				MON-02.5	
AU-6(8)	full text analysis of privileged commands	N/A	N/A	N/A					x										CC7.2		4.3 4.8																		MON-03.3	
AU-6(9)	correlation with information from nontechnical sources	N/A	N/A	N/A					x																															
AU-6(10)	audit level adjustment [Incorporated into AU-6]	N/A	N/A	N/A								AU-6(10)							CC7.2																				MON-02.6	
AU-7	**Audit Record Reduction and Report Generation**	**P-AU-7**	Technical Users	Enhanced			x	x			AU-7	AU-7				AU.3.052	AU.3.052	AU.3.052	CC7.2	COMP:SG3.SP2 TM:SG2.SP2	6.7					164.308(a)(1)(ii)(D)	12.4.1 16.1.7	9.3.3.7			8-602	PR.PT-1 RS.AN-3	3.3.6	3.3.6[a] 3.3.6[b]					MON-06	
AU-7(1)	automatic processing	P-AU-7(1)	Technical Users	Enhanced			x	x			AU-7(1)	AU-7(1)							CC7.2		6.7																		MON-06	
AU-7(2)	automatic search and sort [Incorporated into AU-7(1)]	N/A	N/A	N/A																																				
AU-8	**Time Stamps**	**P-AU-8**	Technical Users	Basic		x	x	x		AU-8	AU-8	AU-8	AU-8		AU.2.043	AU.2.043	AU.2.043	AU.2.043	CC7.2	TM:SG2.SP2	6.1						12.4.4	9.3.3.8			8-602	PR.PT-1	3.3.7	3.3.7[a] 3.3.7[b]				10.4 10.4.1	MON-07 SEA-20	
AU-8(1)	synchronization with authoritative time source	N/A	N/A	N/A							AU-8(1)	AU-8(1)			AU.2.043	AU.2.043	AU.2.043	AU.2.043	CC7.2		6.1												3.3.7						MON-07.1	
AU-8(2)	secondary authoritative time source	N/A	N/A	N/A					x																															
AU-9	**Protection of Audit Information**	**P-AU-9**	Technical Users	Basic		x	x	x		AU-9	AU-9	AU-9	AU-9			AU.3.049	AU.3.049	AU.3.049	CC7.2	TM:SG2.SP2							12.4.2 12.4.3	9.3.3.9			8-602	PR.PT-1	3.3.8	3.3.8[a] 3.3.8[b]				10.5 10.5.1	MON-08	
AU-9(1)	hardware write-once media	N/A	N/A	N/A					x																															
AU-9(2)	store on separate physical systems or components	P-AU-9(2)	Technical Users	Enhanced				x			AU-9(2)	AU-9(2)							CC7.2																				MON-08.1	
AU-9(3)	cryptographic protection	P-AU-9(3)	Technical Users	Enhanced				x				AU-9(3)							CC7.2																				MON-08.3	
AU-9(4)	access by subset of privileged users	P-AU-9(4)	Technical Users	Enhanced			x	x			AU-9(4)	AU-9(4)				AU.3.050	AU.3.050	AU.3.050	CC7.2														3.3.9	3.3.9[a] 3.3.9[b]					MON-08.2	
AU-9(5)	dual authorization	P-AU-9(5)	Technical Users	Enhanced					x										CC7.2																3.1.1e				MON-08.4	
AU-9(6)	read-only access	N/A	N/A	N/A					x																															
AU-9(7)	store on component with different operating system	N/A	N/A	N/A					x																															
AU-10	**Non-repudiation**	**P-AU-10**	Technical Users	Enhanced				x				AU-10							CC7.2	TM:SG2.SP2							13.2.3 14.1.2				8-602	PR.PT-1							MON-09	
AU-10(1)	association of identities	N/A	N/A	N/A					x																															
AU-10(2)	validate binding of information producer identity	N/A	N/A	N/A					x																															
AU-10(3)	chain of custody	N/A	N/A	N/A					x									IR.5.106	CC7.2																				IRO-08	
AU-10(4)	validate binding of information reviewer identity	N/A	N/A	N/A					x																															
AU-10(5)	digital signatures [Incorporated into SI-7]	N/A	N/A	N/A																																				
AU-11	**Audit Record Retention**	**P-AU-11**	Technical Users	Basic	x	x	x	x		AU-11	AU-11	AU-11	AU-11		AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	AU.2.041 AU.2.042	CC7.2	COMP:SG3.SP1 COMP:SG3.SP2							12.4.1 16.1.7	9.3.3.10			8-602	PR.PT-1	3.3.1			500.13		10.7	MON-10	
AU-11(1)	long-term retrieval capability	N/A	N/A	N/A					x																															
AU-12	**Audit Record Generation**	**P-AU-12**	Technical Users	Basic		x	x	x		AU-12	AU-12	AU-12	AU-12		AU.2.041 AU.2.042	AAU.2.041 AU.2.042	AAU.2.041 AU.2.042	AAU.2.041 AU.2.042	CC7.2	TM:SG2.SP2	6.7						12.4.1 12.4.3	9.3.3.11			8-602	PR.PT-1 DE.CM-1	3.3.1 3.3.2						MON-06	
AU-12(1)	system-wide and time-correlated audit trail	P-AU-12(1)	Technical Users	Basic				x				AU-12(1)							CC7.2																				MON-02.7	
AU-12(2)	standardized formats	N/A	N/A	N/A					x																															
AU-12(3)	changes by authorized individuals	P-AU-12(3)	Technical Users	Basic				x				AU-12(3)							CC7.2																				MON-02.8	
AU-12(4)	query parameter audits of personally identifiable information	N/A	N/A	N/A					x																															
AU-13	**Monitoring for Information Disclosure**	**P-AU-13**	Management	Basic					x						IR.2.093	IR.2.093	IR.2.093	IR.2.093	CC7.2	IMC:SG2.SP1 KIM:SG4.SP2									17.04(3)		8-602	PR.PT-1 DE.CM-3							MON-11	
AU-13(1)	use of automated tools	N/A	N/A	N/A					x																															
AU-13(2)	review of monitored sites	N/A	N/A	N/A					x																															
AU-13(3)	unauthorized replication of information	N/A	N/A	N/A					x																															
AU-14	**Session Audit**	N/A	N/A	N/A					x										CC7.2	TM:SG2.SP2	14.9						12.4.1				8-602	PR.PT-1							MON-12	
AU-14(1)	system start-up	N/A	N/A	N/A					x																															
AU-14(2)	capture and record content [Incorporated into AU-14]	N/A	N/A	N/A																																				
AU-14(3)	remote viewing and listening	N/A	N/A	N/A					x																															
AU-15	**Alternate Audit Logging Capability [Incorporated into AU-5(5)]**	N/A	N/A	N/A															CC7.2	CTRL:SG2.SP1 TM:SG5.SP1											8-602	PR.PT-1							MON-13	
AU-16	**Cross-Organizational Audit Logging**	N/A	N/A	N/A					x										CC7.2	COMP:SG3.SP1 EXD:SG3.SP4								9.3.3.12			8-602	PR.PT-1							MON-14	
AU-16(1)	identity preservation	N/A	N/A	N/A					x																															
AU-16(2)	sharing of audit information	N/A	N/A	N/A					x										CC2.3 CC7.2																				MON-14.1	
AU-16(3)	disassociability	N/A	N/A	N/A					x																															
CA-1	**Policy and Procedures**	**P-CA-1**	Management	Basic	x	x	x	x		CA-1	CA-1	CA-1	CA-1						CC5.1 CC5.2	COMP:SG1.SP1						164.308(a)(8)	5.1.1 5.1.2	9.3.4.1			8-200 8-201								IAO-01	
CA-2	**Control Assessments**	**P-CA-2**	Technical Users	Basic	x	x	x	x		CA-2	CA-2	CA-2	CA-2		CA.2.157 CA.2.158	CA.2.157 CA.2.158		CA.2.157 CA.2.158	CC4.1 CC4.2	RISK:SG3.SP1						164.308(a)(2) 164.308(a)(8)	14.2.8 14.2.9	9.3.4.2	17.03(2)(h)		8-610	ID.RA-1 PR.IP-7	3.12.1 3.12.2	3.12.1[a] 3.12.1[b]			622(2)(B)(i)-(iv)		CFG-02.1 CPL-03	
CA-2(1)	independent assessors	P-CA-2(1)	Management	Enhanced			x	x		CA-2(1)	CA-2(1)	CA-2(1)	CA-2(1)						CC4.1 CC4.2																				IAO-02.1	
CA-2(2)	specialized assessments	P-CA-2(2)	Management	Enhanced				x			CA-2(2)	CA-2(2)							CC4.1 CC4.2		18.11																		IAO-02.2	
CA-2(3)	leveraging results from external organizations	P-CA-2(3)	Management	Enhanced					x		CA-2(3)	CA-2(3)							CC4.1 CC4.2																				IAO-02.3	
CA-3	**Information Exchange**	**P-CA-3**	All Users	Basic		x	x	x		CA-3	CA-3	CA-3	CA-3							EXD:SG3.SP4						164.308(b)(1) 164.308(b)(4)	13.1.1 13.1.2	9.3.4.3			8-610	ID.AM-3 DE.AE-1			3.11.4e				NET-05	
CA-3(1)	unclassified national security connections [Moved to SC-7(25)]	N/A	N/A	N/A																																				
CA-3(2)	classified national security system connections [Moved to SC-7(26)]	N/A	N/A	N/A																																				
CA-3(3)	unclassified non-national security system connections [Moved to SC-7(27)]	N/A	N/A	N/A								CA-3(3)	CA-3(3)																										NET-05.1	

R5 # Low / Mod / High	Control Name	Procedures #	Target Audience	Applicability	Privacy	Low	Moderate	High	NOC	Low	Moderate	High	LI-SaaS	Level 1	Level 2	Level 3	Level 4	Level 5	AICPA TSC 2017	CERT RMM	CIS CSC v7.1	FACTA	FAR 52.204-21	Generally Accepted	GLBA	HIPAA	ISO 27002	IRS 1075	MA 201 CMR	NERC CIP	NISPOM	NIST CSF v1.1	NIST 800-171 rev 2	NIST 800-171A	NIST 800-172 [draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2.1	Secure Controls	UK Cyber
CA-3(4)	connections to public networks [Moved to SC-7(28)]	N/A	N/A	N/A																																				
CA-3(5)	restrictions on external system connections [Incorporated into SC-7(5)]	N/A	N/A	N/A							CA-3(5)	CA-3(5)							CC6.6		11.2																	1.2.3 1.3	NET-04.1	
CA-3(6)	transfer authorizations	P-CA-3(6)	Management	Enhanced				x																																
CA-3(7)	transitive information exchanges	N/A	N/A	N/A					x																															
CA-4	Security Certification [Incorporated into CA-2]	N/A	N/A	N/A																																				
CA-5	Plan of Action and Milestones	P-CA-5	Technical Users	Basic	x	x	x	x		CA-5	CA-5	CA-5	CA-5		CA.2.157 CA.2.158	CA.2.157 CA.2.158	CA.2.157 CA.2.158	CA.2.157 CA.2.158	CC4.1 CC4.2	RISK:SG5.SP1								9.3.4.4			8-610		3.12.1 3.12.2	3.12.2[a] 3.12.2[b]					IAO-05	
CA-5(1)	automation support for accuracy and currency	N/A	N/A	N/A					x																															
CA-6	Authorization	P-CA-6	Management	Basic	x	x	x	x		CA-6	CA-6	CA-6	CA-6						CC8.1	EF:SG4.SP1 RISK:SG2.SP1						164.308(a)(2) 164.308(a)(8)	14.2.9	9.3.4.5			8-202 8-610								IAO-07	
CA-6(1)	joint authorization — intra-organization	N/A	N/A	N/A					x																															
CA-6(2)	joint authorization — inter-organization	N/A	N/A	N/A					x																															
CA-7	Continuous Monitoring	P-CA-7	Management	Basic	x	x	x	x		CA-7	CA-7	CA-7	CA-7		CA.2.157 CA.2.158	CA.2.157 CA.2.158	CA.2.157 CA.2.158	CA.2.157 CA.2.158	CC4.1 CC4.2	MON:SG1.SP1 MON:SG1.SP3						164.308(a)(1)(ii)(D)	12.6.1 16.1.3	9.3.4.6			8-202 8-610	ID.RA-1 PR.IP-7	3.12.1 3.12.2	3.12.3			622(2)(B)(iii)		CPL-02	
CA-7(1)	independent assessment	P-CA-7(1)	Management	Enhanced			x	x			CA-7(1)	CA-7(1)							CC4.1 CC4.2																				CPL-02	
CA-7(2)	types of assessments [Incorporated into CA-2]	N/A	N/A	N/A																																				
CA-7(3)	trend analyses	P-CA-7(3)	Management	Enhanced					x			CA-7(3)							CC4.1 CC4.2																				MON-06.2	
CA-7(4)	risk monitoring	P-CA-7(4)	Management	Basic	x	x	x	x																										3.12.3						
CA-7(5)	consistency analysis	N/A	N/A	N/A					x																															
CA-7(6)	automation support for monitoring	N/A	N/A	N/A					x																															
CA-8	Penetration Testing	P-CA-8	Management	Enhanced				x			CA-8	CA-8					CA.4.164	CA.4.164	CC4.1 CC4.2	VAR:SG2.SP1 VAR:SG2.SP2	20.1 20.2										8-610 8-614	ID.RA-1			3.12.1e	500.05		11.3 11.3.1	VPM-07	
CA-8(1)	independent penetration testing agent or team	P-CA-8(1)	Management	Enhanced				x			CA-8(1)	CA-8(1)							CC4.1 CC4.2																				VPM-07.1	
CA-8(2)	red team exercises	P-CA-8(2)	Management	Enhanced					x								CA.4.227	CA.4.227	CC4.1 CC4.2		20.3 20.5																		VPM-10	
CA-8(3)	facility penetration testing	N/A	N/A	N/A					x																															
CA-9	Internal System Connections	P-CA-9	Technical Users	Enhanced		x	x	x		CA-9	CA-9	CA-9	CA-9							COMM:SG2.SP1 TM:SG2.SP2											8-610 8-700								NET-05.2	
CA-9(1)	compliance checks	N/A	N/A	N/A					x																															
CM-1	Policy and Procedures	P-CM-1	Management	Basic	x	x	x	x		CM-1	CM-1	CM-1	CM-1						CC5.1 CC5.2	TM:SG4.SP2	5.5						5.1.1 5.1.2	9.3.5.1			8-311 8-610			3.4.8[a]					CFG-01	
CM-2	Baseline Configuration	P-CM-2	Technical Users	Basic		x	x	x		CM-2	CM-2	CM-2	CM-2		CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CC8.1	TM:SG4.SP2	5.1 5.2						12.1.2 12.1.4	9.3.5.2			8-202 8-311	PR.DS-7 PR.IP-1	3.4.1 3.4.2	3.4.1[a] 3.4.1[b]	3.4.1e 3.4.2e			1.1.1	CFG-02	2-3 2-4
CM-2(1)	reviews and updates [Incorporated into CM-2]	N/A	N/A	N/A							CM-2(1)	CM-2(1)							CC7.3 CC8.1																				CFG-02.1	
CM-2(2)	automation support for accuracy and currency	P-CM-2(2)	Technical Users	Enhanced			x	x			CM-2(2)	CM-2(2)							CC8.1		5.4 5.5														3.4.3e				CFG-02.2	
CM-2(3)	retention of previous configurations	P-CM-2(3)	Technical Users	Basic			x	x			CM-2(3)	CM-2(3)							CC8.1		5.3																		CFG-02.3	
CM-2(4)	unauthorized software [Incorporated into CM-7]	N/A	N/A	N/A																																				
CM-2(5)	authorized software [Incorporated into CM-7]	N/A	N/A	N/A																																				
CM-2(6)	development and test environments	N/A	N/A	N/A					x										CC8.1																			6.4.1	CFG-02.4	
CM-2(7)	configure systems and components for high-risk areas	P-CM-2(7)	Technical Users	Enhanced			x	x			CM-2(7)	CM-2(7)							CC6.6																			1.2.2	CFG-02.5	
CM-3	Configuration Change Control	P-CM-3	Technical Users	Basic			x	x			[illegible]	[illegible]			CM.2.065	CM.2.065	CM.2.065	[illegible]	CC3.4 CC7.1	[illegible]	5.5						12.1.2 12.2.1	9.3.5.3			8-103 8-104	PR.IP-1 PR.IP-3	3.4.3	3.4.3[a] 3.4.3[b]	3.4.1e 3.4.2e				CHG-01 CHG-02	
CM-3(1)	automated documentation, notification, and prohibition of changes	P-CM-3(1)	Technical Users	Basic				x				CM-3(1)							CC8.1																				CHG-02.1	
CM-3(2)	testing, validation, and documentation of changes	P-CM-3(2)	Technical Users	Basic			x	x				CM-3(2)							CC8.1																				CHG-02.2 CHG-06	
CM-3(3)	automated change implementation	N/A	N/A	N/A					x																															
CM-3(4)	security and privacy representatives	P-CM-3(4)	Technical Users	Basic			x	x				CM-3(4)												1.2.6															CHG-02.3	
CM-3(5)	automated security response	P-CM-3(5)	Technical Users	Enhanced					x										[illegible]																3.4.2e				CHG-02.4	
CM-3(6)	cryptography management	P-CM-3(6)	Technical Users	Enhanced				x				[illegible]							[illegible]																				CHG-02.5	
CM-3(7)	review system changes	N/A	N/A	N/A					x										CC8.1																				CHG-02.2	
CM-3(8)	prevent or restrict configuration changes	P-CM-3(8)	Technical Users	Enhanced					x																										3.4.2e					
CM-4	Impact Analysis	P-CM-4	Technical Users	Basic	x	x	x	x		CM-4	CM-4	CM-4	CM-4		CM.2.066	CM.2.066	CM.2.066	CM.2.066	CC3.4 CC7.1	TM:SG3.SP1 TM:SG4.SP3				1.2.6			12.1.2 12.1.4	9.3.5.4			8-103 8-104	PR.IP-1 PR.IP-3	3.4.4	3.4.4				6.4 6.4.5	CHG-03	
CM-4(1)	separate test environments	P-CM-4(1)	Technical Users	Enhanced				x				CM-4(1)							CC8.1																				TDA-08	
CM-4(2)	verification of controls	P-CM-4(2)	Technical Users	Basic			x	x																															IAO-06	
CM-5	Access Restrictions for Change	P-CM-5	Technical Users	Basic		x	x	x			CM-5	CM-5				CM.3.067	CM.3.067	CM.3.067	CC8.1	TM:SG4.SP1							9.2.3 9.4.5	9.3.5.5			8-311 8-610	PR.IP-1	3.4.5	3.4.5[a] 3.4.5[b]					CHG-04 END-03.2	
CM-5(1)	automated access enforcement and audit records	P-CM-5(1)	Technical Users	Enhanced				x			CM-5(1)	CM-5(1)							CC8.1		11.3																		CHG-04.1	
CM-5(2)	review system changes [Incorporated into CM-3(7)]	N/A	N/A	N/A								CM-5(2)							CC8.1																				CHG-02.2	
CM-5(3)	signed components	N/A	N/A	N/A							CM-5(3)	CM-5(3)							CC8.1																				CHG-04.2	
CM-5(4)	dual authorization	P-CM-5(4)	Technical Users	Enhanced					x										CC8.1																3.1.1e				CHG-04.3	
CM-5(5)	privilege limitation for production and operation	P-CM-5(5)	Technical Users	Enhanced					x		CM-5(5)	CM-5(5)							CC8.1																				CHG-04.4	
CM-5(6)	limit library privileges	N/A	N/A	N/A					x										CC8.1																				CHG-04.5	
CM-5(7)	automatic implementation of security safeguards [Incorporated into SI-7]	N/A	N/A	N/A																																				
CM-6	Configuration Settings	P-CM-6	Technical Users	Basic		x	x	x		CM-6	CM-6	CM-6	CM-6		CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CC6.1 CC8.1	TM:SG2.SP1 TM:SG4.SP2	5.1 5.2						12.4.1	9.3.5.6			8-202 8-311	PR.IP-1	3.4.1 3.4.2	3.4.2[a] 3.4.2[b]				1.1 1.1.1	CFG-02	
CM-6(1)	automated management, application, and verification	P-CM-6(1)	Technical Users	Enhanced				x			CM-6(1)	CM-6(1)							CC8.1		5.4 5.5																		CFG-02.2	
CM-6(2)	respond to unauthorized changes	P-CM-6(2)	Technical Users	Basic				x				CM-6(2)							CC7.2		5.5																		CFG-02.8	
CM-6(3)	unauthorized change detection [Incorporated into SI-7]	N/A	N/A	N/A																																				
CM-6(4)	conformance demonstration	N/A	N/A	N/A					x																															
CM-7	Least Functionality	P-CM-7	Technical Users	Basic		x	x	x		CM-7	CM-7	CM-7	CM-7		CM.2.062	CM.2.062	CM.2.062	CM.2.062 SC.5.230	CC6.1	TM:SG2.SP1 TM:SG2.SP2	9.1 9.2						9.1.2 12.4.1	9.3.5.7	17.03(2)(a)			PR.IP-1	3.4.6	3.4.6[a] 3.4.6[b]				1.1.5 1.2.1	CFG-03	1-3
CM-7(1)	periodic review	P-CM-7(1)	Technical Users	Basic			x	x			CM-7(1)	CM-7(1)			CM.2.062	CM.2.062	CM.2.062	CM.2.062	CC7.3														3.4.7						CFG-03.1	1-4
CM-7(2)	prevent program execution	P-CM-7(2)	Technical Users	Basic			x	x			CM-7(2)	CM-7(2)			CM.2.062	CM.2.062	CM.2.062	CM.2.062			8.3												3.4.7						CFG-03.2 SEA-06	1-3
CM-7(3)	registration compliance	N/A	N/A	N/A					x																															
CM-7(4)	unauthorized software	P-CM-7(4)	Technical Users	Enhanced					x							CM.3.069	CM.3.069 CM.4.073	CM.3.069 CM.4.073	CC6.1		2.2 2.7												3.4.8	3.4.8[a] 3.4.8[b]					CFG-03.3	
CM-7(5)	authorized software	P-CM-7(5)	Technical Users	Enhanced			x	x			CM-7(5)	CM-7(5)				CM.3.069	CM.3.069 CM.4.073	CM.3.069 CM.4.073	CC6.1		2.2 2.7												3.4.8	3.4.8[a] 3.4.8[b]					CFG-03.3	
CM-7(6)	confined environments with limited privileges	N/A	N/A	N/A					x																															
CM-7(7)	code execution in protected environments	N/A	N/A	N/A					x																															
CM-7(8)	binary or machine executable code	N/A	N/A	N/A					x										CC8.1																				END-06.7	
CM-7(9)	prohibiting the use of unauthorized hardware	N/A	N/A	N/A					x																															
CM-8	System Component Inventory	P-CM-8	Technical Users	Basic		x	x	x		CM-8	CM-8	CM-8	CM-8		CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CC6.1 CC8.1	ADM:SG1.SP1	1.1 1.4					164.310(d)(1) 164.310(d)(2)(iii)	8.1.1 8.1.2					ID.AM-1 ID.AM-2	3.4.1 3.4.2	3.4.1[d] 3.4.1[e]	3.4.1e 3.11.4e			1.1.2 1.1.3	AST-02 AST-02.3	
CM-8(1)	updates during installation and removal	P-CM-8(1)	Technical Users	Enhanced			x	x			CM-8(1)	CM-8(1)			CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CM.2.061 CM.2.064	CC8.1														3.4.1 3.4.2						AST-02.1	
CM-8(2)	automated maintenance	P-CM-8(2)	Technical Users	Enhanced				x				CM-8(2)					AM.4.226	AM.4.226	CC6.1																3.4.3e				AST-02.9	
CM-8(3)	automated unauthorized component detection	P-CM-8(3)	Technical Users	Enhanced			x	x			CM-8(3)	CM-8(3)							CC7.2 CC7.3		1.1 1.2														3.5.3e				AST-02.2 CFG-05.1	
CM-8(4)	accountability information	P-CM-8(4)	Technical Users	Enhanced				x				CM-8(4)							CC6.1																				AST-03.1	
CM-8(5)	no duplicate accounting of components	N/A	N/A	N/A					x	CM-8(5)	CM-8(5)	CM-8(5)	CM-8(5)						CC8.1		1.1																		AST-02.3	
CM-8(6)	assessed configurations and approved deviations	N/A	N/A	N/A					x										CC8.1		2.10 5.5																		AST-02.4	
CM-8(7)	centralized repository	N/A	N/A	N/A					x																															
CM-8(8)	automated location tracking	N/A	N/A	N/A					x																															
CM-8(9)	assignment of components to systems	N/A	N/A	N/A					x																															
CM-9	Configuration Management Plan	P-CM-9	Technical Users	Basic			x	x			CM-9	CM-9							CC8.1	TM:SG4.SP2	5.5						14.2.4	9.3.5.9				PR.IP-1						1.1.5	CFG-01 CHG-05	
CM-9(1)	assignment of responsibility	N/A	N/A	N/A					x										CC8.1																				CFG-01.1	
CM-10	Software Usage Restrictions	P-CM-10	Management	Basic		x	x	x		CM-10	CM-10	CM-10	CM-10						CC3.2 CC3.3	COMP:SG2.SP1 COMP:SG2.SP2	2.1 2.3						12.5.1 18.1.2	9.3.5.10				DE.CM-3							CFG-04	
CM-10(1)	open-source software	P-CM-10(1)	Technical Users	Enhanced					x		CM-10(1)	CM-10(1)							CC3.2 CC3.3																				CFG-04.1	