NIST 800-53 rev4 Written Information Security Program (WISP) - Applicability Matrix

WISP-LM # NIST 800-53 Rev4	WISP-LMH # NIST 800-53 Rev4	Control Grouping	WISP - Standard Name	NIST 800-53 rev4 LOW	NIST 800-53 rev4 MODERATE	NIST 800-53 rev4 HIGH	NIST 800-53 rev4 No Category	FedRAMP LOW	FedRAMP MODERATE	FedRAMP HIGH	FedRAMP LI-SaaS
CA-1	CA-1	Management	Security Assessment Policy & Procedures	x	x	x		x	x	x	x
CA-2	CA-2	Management	Security Assessments	x	x	x		x	x	x	x
CA-2(1)	CA-2(1)	Management	Security Assessments | Independent Assessors		x	x		x	x	x	x
CA-2(2)	CA-2(2)	Management	Security Assessments | Specialized Assessments			x			x	x	
CA-2(3)	CA-2(3)	Management	Security Assessments | External Organizations				x		x	x	
CA-3	CA-3	Management	System Connections	x	x	x		x	x	x	x
CA-3(3)	CA-3(3)	Management	System Connections | Unclassified Non-National Security System Connections				x		x	x	
CA-3(5)	CA-3(5)	Management	System Connections | Restrictions on External System Connections		x	x			x	x	
CA-4	CA-4	Withdrawn	Security Certification [withdrawn: Incorporated into CA-2]								
CA-5	CA-5	Management	Plan of Action and Milestones (POA&M)	x	x	x		x	x	x	x
CA-6	CA-6	Management	Security Authorization	x	x	x		x	x	x	x
CA-7	CA-7	Management	Continuous Monitoring	x	x	x		x	x	x	x
CA-7(1)	CA-7(1)	Management	Continuous Monitoring | Independent Assessment		x	x			x	x	
Not Included	CA-7(3)	Management	Continuous Monitoring | Trend Analysis				x			x	
CA-8	CA-8	Management	Penetration Testing			x			x	x	
CA-8(1)	CA-8(1)	Management	Penetration Testing | Independent Penetration Agent or Team				x		x	x	
Not Included	CA-8(2)	Management	Penetration Testing | Red Team Exercises				x				
CA-9	CA-9	Management	Internal System Connections	x	x	x		x	x	x	x
PL-1	PL-1	Management	Security Planning Policy & Procedures	x	x	x		x	x	x	x
PL-2	PL-2	Management	System Security Plan (SSP)	x	x	x		x	x	x	x
PL-2(3)	PL-2(3)	Management	System Security Plan (SSP) | Plan / Coordinate with Other Organizational Entities		x	x					
PL-3	PL-3	Withdrawn	System Security Plan Update [withdrawn: Incorporated into PL-2]								
PL-4	PL-4	Management	Rules of Behavior	x	x	x		x	x	x	x
PL-4(1)	PL-4(1)	Management	Rules of Behavior | Social Media & Social Networking Restrictions		x	x			x	x	
PL-5	PL-5	Withdrawn	Privacy Impact Assessment [withdrawn: Incorporated into AR-2]								
PL-6	PL-6	Withdrawn	Security-Related Activity Planning [withdrawn - incorporated in PL-2]								
PL-7	PL-7	Management	Security Concept Of Operations				x				
PL-8	PL-8	Management	Information Security Architecture		x	x			x	x	
Not Included	PL-8(1)	Management	Information Security Architecture | Defense In Depth				x				
Not Included	PL-8(2)	Management	Information Security Architecture | Supplier Diversity				x				
PL-9	PL-9	Management	Central Management				x				
PM-1	PM-1	Management	Information Security Program Plan				x				
PM-2	PM-2	Management	Senior Information Security Officer				x				
PM-3	PM-3	Management	Information Security Resources				x				
PM-4	PM-4	Management	Plan of Action & Milestones (POA&M) (Vulnerability Remediation Process)				x				
PM-5	PM-5	Management	Information System Inventory				x				
PM-6	PM-6	Management	Information Security Measures of Performance				x				
PM-7	PM-7	Management	Enterprise Architecture				x				
PM-8	PM-8	Management	Critical Infrastructure Plan (CIP)				x				
PM-9	PM-9	Management	Risk Management Strategy				x				
PM-10	PM-10	Management	Security Authorization Process				x				
PM-11	PM-11	Management	Mission / Business Process Definition				x				
PM-12	PM-12	Management	Insider Threat Program				x				
PM-13	PM-13	Management	Information Security Workforce				x				
PM-14	PM-14	Management	Testing, Training, and Monitoring				x				
PM-15	PM-15	Management	Contacts with Security Groups and Associations				x				
PM-16	PM-16	Management	Threat Awareness Program				x				
RA-1	RA-1	Management	Risk Assessment Policy & Procedures	x	x	x		x	x	x	x
RA-2	RA-2	Management	Security Categorization	x	x	x		x	x	x	x
RA-3	RA-3	Management	Risk Assessment	x	x	x		x	x	x	x
RA-4	RA-4	Withdrawn	Risk Assessment Update [withdrawn: incorporated into RA-3]								
RA-5	RA-5	Management	Vulnerability Scanning	x	x	x		x	x	x	x
RA-5(1)	RA-5(1)	Management	Vulnerability Scanning | Update Tool Capability		x	x			x	x	
RA-5(2)	RA-5(2)	Management	Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified		x	x			x	x	
RA-5(3)	RA-5(3)	Management	Vulnerability Scanning | Bredth / Depth of Coverage				x		x	x	
Not Included	RA-5(4)	Management	Vulnerability Scanning | Discoverable Information			x				x	
RA-5(5)	RA-5(5)	Management	Vulnerability Scanning | Privileged Access		x	x			x	x	
RA-5(6)	RA-5(6)	Management	Vulnerability Scanning | Automated Trend Analysis				x		x	x	
RA-5(8)	RA-5(8)	Management	Vulnerability Scanning | Review Historic Audit Logs				x		x	x	
Not Included	RA-5(10)	Management	Vulnerability Scanning | Correlate Scanning Information				x			x	
RA-6	RA-6	Management	Technical Surveillance Countermeasures Survey				x				
SA-1	SA-1	Management	System & Services Acquisition Policy & Procedures	x	x	x		x	x	x	x

WISP-LMH # NIST 800-53 Rev4	AICPA TSC 2017 (SOC 2)	CERT RMM v1.2	CIS CSC v7.1	DoD CMMC 0.6	FACTA	FAR 52.204-21	Generally Accepted Privacy Principles (GAPP)	GLBA	HIPAA
CA-1	CC5.1 CC5.2	COMP:SG1.SP1							164.308(a)(8)
CA-2	CC4.1 CC4.2	RISK:SG3.SP1		RM.3.144 CA2.157 CA2.158 CA2.159 CA3.161					164.308(a)(2) 164.308(a)(8)
CA-2(1)	CC4.1 CC4.2								
CA-2(2)	CC4.1 CC4.2		18.11						
CA-2(3)	CC4.1 CC4.2								
CA-3		EXD:SG3.SP4							164.308(b)(1) 164.308(b)(4) 164.314(a)(2)(i)
CA-3(3)									
CA-3(5)	CC6.6		11.2						
CA-4									
CA-5	CC4.1 CC4.2	RISK:SG5.SP1		RM.3.146 CA2.157 CA2.158 CA2.159 CA3.161					
CA-6	CC8.1	EF:SG4.SP1 RISK:SG2.SP1							164.308(a)(2) 164.308(a)(8)
CA-7	CC4.1 CC4.2	MON:SG1.SP1 MON:SG1.SP3		CA2.157 CA2.158 CA2.159 CA3.161					164.308(a)(1)(ii)(D) 164.308(a)(8)
CA-7(1)	CC4.1 CC4.2								
CA-7(3)	CC4.1 CC4.2								
CA-8	CC4.1 CC4.2	VAR:SG2.SP1 VAR:SG2.SP2	20.1 20.2 20.3 20.4 20.5 20.6 20.7						
CA-8(1)	CC4.1 CC4.2								
CA-8(2)	CC4.1 CC4.2		20.3 20.5 20.7						
CA-9		COMM:SG2.SP1 TM:SG2.SP2							
PL-1	CC3.2 CC3.3 CC5.1 CC5.2	EF:SG3.SP3 EF:SG4.SP1							[illegible]
PL-2	CC3.2 CC3.3	AM:SG1.SP1 EF:SG2.SP1 TM:SG1.SP1 TM:SG2.SP1 TM:SG2.SP2	11.2 12.1 12.9	CA.2.157 CA.2.158 CA.2.159 CA.3.161					[illegible]
PL-2(3)	CC3.2 CC3.3								
PL-3									
PL-4		AM:SG1.SP1							
PL-4(1)				SC.3.193					
PL-5									
PL-6									
PL-7	CC3.2 CC3.3	EF:SG2.SP1							
PL-8	CC3.3 CC5.1 CC5.2	EF:SG2.SP1 EXD:SG1.SP1 RTSE:SG1.SP3							
PL-8(1)	CC6.1								
PL-8(2)	CC8.1								
PL-9	CC1.5	EF:SG2.SP2							
PM-1	CC1.2 CC5.3	EF:SG2.SP1 EF:SG2.SP2					8.2.1	6801(b)(1)	
PM-2	CC1.2						1.1.2	Safeguards Rule	
PM-3		EF:SG3.SP1							
PM-4		EC:SG3.SP2 EF:SG2.SP1 EF:SG2.SP2 PM:SG2.SP2 RISK:SG5.SP1 TM:SG3.SP2		RM.3.146					
PM-5		ADM:SG1.SP1 TM:SG1.SP1	1.4 1.5 1.6 2.1 2.5 2.6						
PM-6	CC2.1 CC2.2 CC2.3	AM:GG2.GP8 EF:SG4.SP2 MA:SG1.SP1 MON:SG1.SP1 MON:SG1.SP3					[illegible]		
PM-7		CTRL:SG2.SP1 EC:SG3.SP1 EC:SG3.SP2 EF:SG1 EF:SG1.SP2 EF:SG1.SP3 KIM:SG3.SP1 PM:SG2.SP1 PM:SG2.SP2 RRD:SG2.SP2 RRM:SG1.SP1 RRM:SG1.SP5 RTSE:SG2.SP2 SC:SG1.SP2 TM:SG2.SP2 TM:SG3.SP1							
PM-8	CC3.1	EF:SG1.SP1						6801(b)(3)	
PM-9	CC9.1	EF:SG1.SP1 RISK:SG1.SP2 RISK:SG2.SP1 RISK:SG2.SP2 RISK:SG3.SP1 [illegible] RISK:SG4.SP3 RISK:SG5.SP1 RISK:SG5.SP2 RISK:SG6.SP1		RM.3.144 RM.3.146				6801(b)(2)	
PM-10		TM:SG3.SP1 TM:SG3.SP2							
PM-11		ADM:SG2.SP1 [illegible] PM:SG3.SP2 PM:SG3.SP4 PM:SG3.SP5 SC:SG1.SP1 SC:SG3.SP1							
PM-12		IMC:SG1.SP1							
PM-13		[illegible]	17.2 17.3 17.4 17.5 17.6 17.7 17.8						
PM-14		MON:SG1.SP1 OPD:SG1.SP1 OTA:SG4.SP1					8.2.7		
PM-15		COMM:SG2.SP1 OTA:SG2.SP1	19.5						164.308(a)(5)(ii)(A) 164.308(a)(5)(i)
PM-16		COMM:SG1.SP1 OPD:SG1.SP1		SA.3.169					
RA-1	CC3.2 CC3.3 CC9.1 CC9.2								164.316(a)
RA-2	CC3.2 CC3.3	ADM:SG1.SP1 ADM:SG2.SP1 RISK:SG1.SP1							164.308(a)(7)(ii)(E)
RA-3	CC3.2 CC3.3	RISK:SG2.SP1 RISK:SG2.SP2 RISK:SG3.SP1 RISK:SG3.SP2 RISK:SG4.SP1 RISK:SG4.SP2 RISK:SG4.SP3 RISK:SG5.SP1	19.8	RM.2.141 RM.3.144 RM.3.146			1.2.4	Safeguards Rule	164.316(a)
RA-4									
RA-5	CC4.1 CC4.2	MON:SG2.SP1 MON:SG2.SP2 MON:SG2.SP3 MON:SG2.SP4 VAR:SG2.SP1 VAR:SG2.SP2 VAR:SG2.SP3 VAR:SG3.SP1	3.1 3.2 9.3 12.2	RM.2.142 RM.2.143					
RA-5(1)	CC4.1 CC4.2								
RA-5(2)	CC4.1 CC4.2								
RA-5(3)	CC4.1 CC4.2								
RA-5(4)	CC4.1 CC4.2								
RA-5(5)	CC4.1 CC4.2		3.3	RM.2.142					
RA-5(6)	CC4.1 CC4.2		3.6						
RA-5(8)	CC4.1 CC4.2								
RA-5(10)	CC4.1 CC4.2								
RA-6	CC4.1 CC4.2	IMC:SG2.SP1 VAR:SG2.SP1		IR.2.093					
SA-1	CC5.1 CC5.2		18.1 18.4 18.5 18.6						

WISP-LMH # NIST 800-53 Rev4	ISO 27002 v2013	IRS 1075	MA 201 CMR 17.00	NERC CIP	NISPOM	NIST CSF v1.1	NIST 800-171 rev 1	NIST 800-171B [initial draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2	Secure Controls Framework (SCF)	UK Cyber Essentials	Target Audience	Applicability
CA-1	5.1.1, 5.1.2, 6.1.1, 18.2.1, 6.1.1, 12.1.1, 18.1.1 & 18.2.2	9.3.4.1			8-200 8-201 8-202 8-610							IAO-01		Management	Basic
CA-2	14.2.8, 14.2.9, 16.1.3, 18.2.1, 18.2.2 & 18.2.3	9.3.4.2	17.03(2)(h)		8-610	ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3	3.12.1 3.12.2 3.12.3 3.12.4			622(2)(B)(i)-(iv)		CPL-03 CPL-03.2 IAO-02 IAO-06 PRM-04		Technical Users	Basic
CA-2(1)												IAO-02.1		Management	Enhanced
CA-2(2)												IAO-02.2		Management	Enhanced
CA-2(3)												IAO-02.3		Management	Enhanced
CA-3	15.1.2, 13.1.1, 13.1.2, 13.2.1 & 13.2.2	9.3.4.3			8-610	ID.AM-3 & DE.AE-1						NET-05		All Users	Basic
CA-3(3)												NET-05.1		Management	Enhanced
CA-3(5)											1.2.3, 1.3, 1.3.3 & 1.3.5	NET-04.1		Technical Users	Basic
CA-4														N/A	N/A
CA-5		9.3.4.4			8-610		3.12.1 3.12.2 3.12.3 3.12.4					IAO-05		Technical Users	Basic
CA-6	14.2.9	9.3.4.5			8-202 8-610 8-614							IAO-07		Management	Basic
CA-7	18.2.1, 12.6.1, 16.1.3, 18.2.2 & 18.2.3	9.3.4.6			8-202 8-610 8-614	ID.RA-1, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.CO-3 & RS.MI-3	3.12.1 3.12.2 3.12.3 3.12.4			622(2)(B)(iii)		CPL-02		Management	Basic
CA-7(1)												CPL-02		Management	Enhanced
CA-7(3)												MON-06.2		Management	Enhanced
CA-8					8-610 8-614	ID.RA-1		3.12.1e	500.05		11.3-11.3.3	VPM-07		Management	Enhanced
CA-8(1)												VPM-07.1		Management	Enhanced
CA-8(2)												VPM-10		Management	Enhanced
CA-9					8-610 8-700							NET-05.2		Technical Users	Enhanced
PL-1	5.1.1, 5.1.2, 6.1.1, [illegible]	9.3.12.1			8-101 8-311	ID.AM-3						CPL-01 PRM-01 TDA-01		Management	Basic
PL-2	[illegible] 6.1.2	9.3.12.2	17.03(2)(b)(i)		8-311 8-610	PR.IP-7 & DE.DP-5	3.12.1 3.12.2 3.12.3 3.12.4	3.11.4e				AST-04 IAO-03		Technical Users	Basic
PL-2(3)												IAO-03.1		Technical Users	Basic
PL-3														N/A	N/A
PL-4	[illegible] 5.1.2, 8.1.3, 7.2.1, [illegible]	9.3.12.3	17.03(2)(b)(2)		8-103						4.2, 12.3, 12.3.1, 12.3.2, 12.3.5-6, 12.3.10 & 12.4	HRS-05.1		All Users	Basic
PL-4(1)												HRS-05.2		All Users	Basic
PL-5						ID.RA-4								N/A	N/A
PL-6														N/A	N/A
PL-7	14.1.1				8-610							OPS-02		Management	Basic
PL-8	14.1.1					ID.AM-3 & PR.IP-2		3.13.1e				SEA-02		Management	Basic
PL-8(1)												SEA-03		Technical Users	Enhanced
PL-8(2)												TDA-03.1		Technical Users	Enhanced
PL-9												GOV-04 SEA-01.1		Management	Basic
PM-1	5.1.1, 5.1.2 & 6.1.1		17.03(1), 17.04 & 17.03(2)(b)(2)		8-100	ID.GV-1 & ID.GV-2			500.02 500.03		12.1 & 12.1.1	GOV-01 GOV-02 GOV-03		Management	Basic
PM-2	6.1.1	9.3.18.1	17.03(2)(a)		8-101	ID.AM-6 & ID.GV-2			500.04	622(2)(d)(A)(i)	12.5-12.5.5	GOV-04		Management	Basic
PM-3												PRM-02		Management	Basic
PM-4			17.03(2)(j)		8-311	ID.RA-6				622(2)(d)(B)(iii)		IAO-05 VPM-02		Management	Basic
PM-5	8.1.1 & 8.1.2				8-311	ID.AM-1 & ID.AM-2					12.3.3, 12.3.4 & 12.3.7	AST-01 AST-02		Management	Basic
PM-6			17.03(2)(j)		8-311	ID.AM-2 & PR.IP-7				622(2)(d)(A)(vi) & 622(2)(d)(B)(iii)		GOV-04 GOV-05		Management	Basic
PM-7					8-103						2.2	SEA-02		Management	Basic
PM-8					8-104	ID.BE-2, ID.BE-4, ID.GV-3 & ID.RM-3					12.1	BCD-01 CPL-01		Management	Basic
PM-9	18.2.1 & 17.1.1		17.03(2)(b)		8-103	ID.GV-4, ID.RA-3, ID.RA-4, ID.RA-6, ID.RM-1, ID.RM-2 & ID.RM-3			500.09	622(2)(d)(A)(ii)	12.2	RSK-01		Management	Basic
PM-10	6.1.1				8-303							IAO-01		Management	Basic
PM-11					8-303	ID.AM-6, ID.BE-3, ID.GV-4, ID.RA-4 & ID.RM-3						PRM-06		Management	Basic
PM-12						ID.RA-3						THR-04		Management	Enhanced
PM-13	7.2.2				8-103 8-307	PR.AT-1, PR.AT-2, PR.AT-4 & PR.AT-5			500.14			HRS-03 SAT-01		Management	Enhanced
PM-14	7.2.2				8-302	PR.IP-10, DE.DP-1, DE.DP-2, DE.DP-3 & DE.DP-5						CPL-02		Management	Basic
PM-15					8-101	ID.RA-2 & RS.CO-5			500.10		5.1.2 6.1 6.2 12.4	GOV-07		Management	Basic
PM-16	6.1.4				8-103	ID.RA-2, ID.RA-3 & ID.RA-5		3.11.1e 3.14.6e			12.6	THR-01		Management	Enhanced
RA-1	5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.1 & 18.2.2	9.3.14.1	17.03(2)(b)		8-610				500.09			RSK-01		Management	Basic
RA-2	8.2.1 & 14.1.1				8-402	ID.AM-5, ID.RA-4 & ID.RA-5					9.6.1	RSK-02		Management	Basic
RA-3	12.6.1 & 17.1.1	9.3.14.2	17.03(2)(b) 17.03(2)(i) 17.03(2)(b)(3)		8-402	ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, PR.IP-12, DE.AE-4 & RS.MI-3	3.11.1	3.11.5e 3.11.6e	500.09	622(2)(A)(ii) 622(2)(A)(iv)	12.2	RSK-04		Management	Basic
RA-4											6.1			N/A	N/A
RA-5	12.6.1 & 18.2.3	9.3.14.3			8-614	ID.RA-1, PR.IP-12, DE.CM-8, DE.DP-4, DE.DP-5, RS.CO-3 & RS.MI-3	3.11.2 3.11.3		500.05	622(2)(B)(iii) & 622(2)(d(A)(iii)	11.2, 11.2.2 & 11.2.3	VPM-06		Management	Basic
RA-5(1)									500.05			VPM-06.1		Technical Users	Enhanced
RA-5(2)												VPM-06.9		Technical Users	Enhanced
RA-5(3)												VPM-06.1		Technical Users	Basic
RA-5(4)												VPM-06.2		Technical Users	Enhanced
RA-5(5)							3.11.2					VPM-06.8		Technical Users	Enhanced
RA-5(6)												VPM-06.3		Technical Users	Basic
RA-5(8)												VPM-06.4		Technical Users	Basic
RA-5(10)												VPM-06.5		Technical Users	Enhanced
RA-6												VPM-08		Management	Enhanced
SA-1	5.1.1, 5.1.2, 6.1.1, 12.1.1, 14.2.7, 18.1.1 & 18.2.2	9.3.15.1							500.11			TDA-01 TDA-06		Management	Basic

EXAMPLE

EXAMPLE

WISP-LM # NIST 800-53 Rev4	WISP-LMH # NIST 800-53 Rev4	Control Grouping	WISP - Standard Name	NIST 800-53 rev4 LOW	NIST 800-53 rev4 MODERATE	NIST 800-53 rev4 HIGH	NIST 800-53 rev4 No Category	FedRAMP LOW	FedRAMP MODERATE	FedRAMP HIGH	FedRAMP LI-SaaS
SA-2	SA-2	Management	Allocation of Resources	x	x	x		x	x	x	x
SA-3	SA-3	Management	System Develop Life Cycle (SDLC)	x	x	x		x	x	x	x
SA-4	SA-4	Management	Acquisition Process	x	x	x		x	x	x	x
SA-4(1)	SA-4(1)	Management	Acquisition Process | Functional Properties Of Security Controls		x	x			x	x	
SA-4(2)	SA-4(2)	Management	Acquisition Process | Design & Implementation of Security Controls		x	x			x	x	
Not Included	SA-4(3)	Management	Acquisition Process | Development Methods, Techniques & Processes				x				
Not Included	SA-4(6)	Management	Acquisition Process | Use of Information Assurance Products				x				
SA-4(8)	SA-4(8)	Management	Acquisition Process | Continuous Monitoring Plan				x		x	x	
SA-4(9)	SA-4(9)	Management	Acquisition Process | Functions / Ports / Protocols / Services in Use		x	x			x	x	
SA-4(10)	SA-4(10)	Management	Acquisition Process | Use of Approved PIV Products	x	x	x			x	x	x
SA-5	SA-5	Management	Information System Documentation	x	x	x		x	x	x	x
SA-6	SA-6	Withdrawn	Software Usage Restrictions [withdrawn - incorporated in CM-10 & SI-7]								
SA-7	SA-7	Withdrawn	User-Installed Software [withdrawn - incorporated in CM-11 & SI-7]								
SA-8	SA-8	Management	Secure Engineering Principles		x	x			x	x	
SA-9	SA-9	Management	External Information Systems	x	x	x		x	x	x	x
SA-9(1)	SA-9(1)	Management	External Information System Services | Risk Assessments & Organizational Approvals				x		x	x	
SA-9(2)	SA-9(2)	Management	External Information System Services | Identification Of Functions, Ports, Protocols & Services		x	x			x	x	
Not Included	SA-9(3)	Management	External Information System Services | Maintain Trust Relationship with Providers				x				
SA-9(4)	SA-9(4)	Management	External Information System Services | Consistent Interests of Consumers and Providers				x		x	x	
SA-9(5)	SA-9(5)	Management	External Information System Services | Processing, Storage and Service Location				x		x	x	
SA-10	SA-10	Management	Developer Configuration Management		x	x			x	x	
SA-10(1)	SA-10(1)	Management	Developer Configuration Management | Software / Firmware Integrity Verification				x		x	x	
SA-11	SA-11	Management	Developer Security Testing		x	x			x	x	
SA-11(1)	SA-11(1)	Management	Developer Security Testing | Static Code Analysis				x		x	x	
SA-11(2)	SA-11(2)	Management	Developer Security Testing | Threat Analysis & Flaw Remediation				x		x	x	
SA-11(8)	SA-11(8)	Management	Developer Security Testing | Dynamic Code Analysis				x		x	x	
SA-12	SA-12	Management	Supply Chain Protection			x				x	
Not Included	SA-12(1)	Management	Supply Chain Protection | Acquisition Strategies, Tools & Methods				x				
Not Included	SA-12(2)	Management	Supply Chain Protection | Supplier Reviews				x				
Not Included	SA-12(5)	Management	Supply Chain Protection | Liability of Harm				x				
Not Included	SA-12(10)	Management	Supply Chain Protection | Validate as Genuine & Not Altered				x				
Not Included	SA-12(15)	Management	Supply Chain Protection | Processes to Address Weaknesses or Deficiencies				x				
SA-13	SA-13	Management	Trustworthiness				x				
SA-14	SA-14	Management	Criticality Analysis				x				
SA-15	SA-15	Management	Development Process, Standards, and Tools			x				x	
Not Included	SA-15(9)	Management	Development Process, Standards, and Tools | Use of Live Data				x				
SA-16	SA-16	Management	Developer-Provided Training			x				x	
SA-17	SA-17	Management	Developer Security Architecture and Design			x				x	
SA-18	SA-18	Management	Tamper Resistance and Detection				x				
Not Included	SA-18(2)	Management	Tamper Resistance and Detection | Inspection of Information Systems, Components or Devices				x				
SA-19	SA-19	Management	Component Authenticity				x				
Not Included	SA-19(1)	Management	Component Authenticity | Anti-Counterfeit Training				x				
Not Included	SA-19(3)	Management	Component Authenticity | Component Disposal				x				
SA-20	SA-20	Management	Customized Development of Critical Components				x				
SA-21	SA-21	Management	Developer Screening				x				
SA-22	SA-22	Management	Unsupported System Components				x				
Not Included	SA-22(1)	Management	Unsupported System Components | Alternate Sources for Continued Support				x				
AT-1	AT-1	Operational	Security Awareness & Training Policy & Procedures	x	x	x		x	x	x	[illegible]
AT-2	AT-2	Operational	Security Awareness Training	x	x	x		x	x	x	x
Not Included	AT-2(1)	Operational	Security Awareness Training | Practical Exercises				x				
AT-2(2)	AT-2(2)	Operational	Security Awareness Training | Insider Threat		x	x			x	x	
AT-3	AT-3	Operational	Roles-Based Security Training	x	x	x		x	x	x	x
Not Included	AT-3(3)	Operational	Roles-Based Security Training | Practical Exercises				x			x	
Not Included	AT-3(4)	Operational	Roles-Based Security Training | Suspicious Communications & Anomalous System Behavior				x			x	
AT-4	AT-4	Operational	Security Training Records	x	x	x		x	x	x	x
AT-5	AT-5	Withdrawn	Security Industry Alerts & Notification Process [withdrawn: Incorporated into PM-15]								
CP-1	CP-1	Operational	Contingency Planning Policy & Procedures	x	x	x		x	x	x	x
CP-2	CP-2	Operational	Contingency Plan	x	x	x		x	x	x	x
CP-2(1)	CP-2(1)	Operational	Contingency Plan | Coordinate with Related Plans		x	x			x	x	
CP-2(2)	CP-2(2)	Operational	Contingency Plan | Capacity Planning			x			x	x	
CP-2(3)	CP-2(3)	Operational	Contingency Plan | Resume Essential Missions / Business Functions		x	x			x	x	
Not Included	CP-2(4)	Operational	Contingency Plan | Resume All Missions / Business Functions			x				x	
Not Included	CP-2(5)	Operational	Contingency Plan | Continue Essential Missions / Business Functions			x				x	
Not Included	CP-2(6)	Operational	Contingency Plan | Alternate Processing / Storage Site				x				
CP-2(8)	CP-2(8)	Operational	Contingency Plan | Identify Critical Assets		x	x			x	x	
CP-3	CP-3	Operational	Contingency Training	x	x	x		x	x	x	x
Not Included	CP-3(1)	Operational	Contingency Training | Simulated Events			x				x	
CP-4	CP-4	Operational	Contingency Plan Testing	x	x	x		x	x	x	x
CP-4(1)	CP-4(1)	Operational	Contingency Plan Testing | Coordinate with Related Plans		x	x			x	x	
Not Included	CP-4(2)	Operational	Contingency Plan Testing | Alternate Processing Site			x				x	
CP-5	CP-5	Withdrawn	Contingency Plan Update [withdrawn: Incorporated into CP-2]								
CP-6	CP-6	Operational	Alternate Storage Site		x	x			x	x	
CP-6(1)	CP-6(1)	Operational	Alternate Storage Site | Separation from Primary Site		x	x			x	x	
Not Included	CP-6(2)	Operational	Alternate Storage Site | Recovery Time / Point Objectives			x				x	
CP-6(3)	CP-6(3)	Operational	Alternate Storage Site | Accessibility		x	x			x	x	
CP-7	CP-7	Operational	Alternate Processing Site		x	x			x	x	
CP-7(1)	CP-7(1)	Operational	Alternate Processing Site | Separation from Primary Site		x	x			x	x	
CP-7(2)	CP-7(2)	Operational	Alternate Processing Site | Accessibility		x	x			x	x	
CP-7(3)	CP-7(3)	Operational	Alternate Processing Site | Priority of Service		x	x			x	x	
Not Included	CP-7(4)	Operational	Alternate Processing Site | Preparation for Use			x				x	
Not Included	CP-7(6)	Operational	Alternate Processing Site | Inability to Return To Primary Site				x				
CP-8	CP-8	Operational	Telecommunications Services		x	x			x	x	
CP-8(1)	CP-8(1)	Operational	Telecommunications Services | Priority-of-Service Provisions		x	x			x	x	
CP-8(2)	CP-8(2)	Operational	Telecommunications Services | Single Points of Failure		x	x			x	x	
Not Included	CP-8(3)	Operational	Telecommunications Services | Separation of Primary / Alternate Providers			x				x	
Not Included	CP-8(4)	Operational	Telecommunications Services | Provider Contingency Plan			x				x	

WISP-LMH # NIST 800-53 Rev4	AICPA TSC 2017 (SOC 2)	CERT RMM v1.2	CIS CSC v7.1	DoD CMMC 0.6	FACTA	FAR 52.204-21	Generally Accepted Privacy Principles (GAPP)	GLBA	HIPAA	ISO 27002 v2013	IRS 1075	MA 201 CMR 17.00	NERC CIP
SA-2	CC3.3	EXD:SG3.SP1 EXD:SG3.SP3 RRD:SG2.SP1 RRM:SG1.SP2								12.1.3	9.3.15.2		
SA-3	CC8.1	EXD:SG3.SP3 EXD:SG3.SP4 EXD:SG4.SP1 EXD:SG4.SP2 RTSE:SG2.SP2								6.1.1 & 14.1.1	9.3.15.3		
SA-4		EXD:SG3.SP4 RTSE:SG1.SP1 RTSE:SG1.SP2 RTSE:SG1.SP3 RTSE:SG1.SP4 RTSE:SG1.SP5							164.314(a)(2)(i)	14.2.9 & 14.2.7	9.3.15.4		
SA-4(1)													
SA-4(2)													
SA-4(3)													
SA-4(6)			18.4 18.5										
SA-4(8)			18.8										
SA-4(9)													
SA-4(10)													
SA-5	CC1.4 CC6.1	TM:SG4.SP2	12.1 12.9							12.1.1, 16.1.3 & 18.1.3	9.3.15.5		
SA-6													
SA-7													
SA-8			5.1 5.2 5.3 5.5 6.2 8.3 8.4 8.5 8.6 9.1 9.2 11.1 14.8 15.6 15.7 15.8	SC.3.180 SC.1.175		(b)(1)(x)				10.4.2 ,14.1.1 & 14.2.5	9.3.15.6		
SA-9	CC4.1 CC4.2	EXD:SG3.SP4 EXD:SG4.SP1							164.308(b)(1) 164.308(b)[illegible]	6.1.1, 13.2.4, 15.1.2, 7.2.1, 15.2.1, 13.2.2 & 14.2.7	9.3.15.7	17.03(2)(f)(1)	
SA-9(1)								[illegible]				17.03(2)(f)(2)	
SA-9(2)													
SA-9(3)	CC3.2 CC3.3												
SA-9(4)	CC3.2 CC3.3												
SA-9(5)	CC6.4 CC6.5												
SA-10	CC8.1	TM:SG4.SP2 TM:SG4.SP3 VAR:SG2.SP2 VAR:SG2.SP3 VAR:SG3.SP1								12.1.2, 12.1.4, 15.2.2, 14.2.9, 9.4.5, 14.2.2 & 14.2.7	9.3.15.8	17.03(2)(d)(B)(i)	
SA-10(1)													
SA-11		EXD:SG3.SP4 RTSE:SG1.SP4 RTSE:SG1.SP5 VAR:SG2.SP2 VAR:SG2.SP3 VAR:SG3.SP1 VAR:SG4.SP1	18.2 18.4 18.8	CA.3.162						18.2.1, 14.2.9, 14.2.7 & 16.1.3	9.3.15.9	17.03(2)(d)(B)(i)	
SA-11(1)			18.7										
SA-11(2)													
SA-11(8)			18.7	CA.3.162									
SA-12		EXD:SG3.SP1 EXD:SG3.SP2 EXD:SG3.SP3 EXD:SG3.SP4 EXD:SG4.SP1 EXD:SG4.SP2 RTSE:SG2.SP1 RTSE:SG2.SP2 RTSE:SG3.SP1 RTSE:SG3.SP2								14.2.7			
SA-12(1)													
SA-12(2)													
SA-12(5)													
SA-12(10)			18.4										
SA-12(15)	CC8.1												
SA-13		EXD:SG3.SP2 EXD:SG3.SP4 EXD:SG4.SP1 RRD:SG2.SP1 RRD:SG3.SP2 RRD:SG3.SP3 RTSE:SG1.SP2 TM:SG2.SP1								14.2.7			
SA-14		RTSE:SG2.SP1 RTSE:SG2.SP2 RTSE:SG3.SP1 RTSE:SG3.SP2 TM:SG1.SP1											
SA-15	CC3.3 CC8.1	CTRL:SG2.SP1 IMC:SG1.SP1 MASG1.SP2 [illegible]	18.1 [illegible]							14.3.1 & 14.2.7			
SA-15(9)	CC8.1											17.03(2)(d)(B)(i)	
SA-16	CC1.4	[illegible]SG3.SP1								7.2.2			
SA-17		[illegible]SG1.SP3											
SA-18		[illegible]											
SA-18(2)	CC8.1												
SA-19	CC6.8	[illegible].SP1	18.4										
SA-19(1)	[illegible]												
SA-19(3)	[illegible] CC6.5												
SA-20		[illegible]		RM.3.144									
SA-21	CC1.1	[illegible]								7.1.1			
SA-22		[illegible]	2.2 2.7 2.8 2.9 18.3	RM.3.147							9.3.15.10		
SA-22(1)	[illegible]			RM.3.147									
AT-1	[illegible]	OPD:SG[illegible] OTA:SG[illegible].SP1 OTASG1.SP3 [illegible]ASG3.SP1 OTASG3.SP2 OTASG3.SP3	17.2 17.3 17.4 17.5 17.6 17.7 17.8 17.9						164.308(a)(5)(i)	5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.1 & 18.2.2	9.3.2.1		
AT-2		OTA:SG2.SP1	17.3 17.9	AT.2.056 AT.2.057					164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B)	7.2.2 & 12.2.1	9.3.2.2	17.04(8) & 17.03(2)(b)(1)	
AT-2(1)													
AT-2(2)				AT.3.058									
AT-3		OTA:SG4.SP1	17.2 17.9	AT.2.056 AT.2.057					164.308(a)(5)(i)	7.2.2 & 12.2.1	9.3.2.3	17.04(8)	
AT-3(3)													
AT-3(4)													
AT-4		OTA:SG2.SP2 OTA:SG4.SP2							164.308(a)(5)(i)		9.3.2.4		
AT-5			19.5										
CP-1	CC3.2 CC3.3 CC5.1 CC5.2	SC:SG1.SP1							164.308(a)(7)(i)	5.1.1, 5.1.2, 6.1.1, 12.1.1, 17.1.2, 17.1.2, 18.1.1 & 18.2.2	9.3.6.1		
CP-2	CC3.2 CC3.3	SC:SG2.SP1 SC:SG3.SP2 SC:SG3.SP3 SC:SG7.SP2							164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.310(a)(2)(i) 164.312(a)(2)(ii)	6.1.1, 11.1.3, 12.1.3, 17.1.2, 17.1.1 & 17.1.3	9.3.6.2		
CP-2(1)	CC3.2 CC3.3												
CP-2(2)	A1.1												
CP-2(3)	CC3.2 CC3.3												
CP-2(4)	CC3.2 CC3.3												
CP-2(5)	CC3.2 CC3.3												
CP-2(6)	CC3.2 CC3.3												
CP-2(8)	CC3.2 CC3.3												
CP-3	CC1.4	SC:SG3.SP5 SC:SG5.SP3							164.308(a)(7)(ii)(D)	7.2.2	9.3.6.3		
CP-3(1)	CC1.4												
CP-4	A1.3	SC:SG5.SP2 SC:SG5.SP3 SC:SG5.SP4							164.308(a)(7)(ii)(D)	17.1.2 & 17.1.3	9.3.6.4		
CP-4(1)	A1.3												
CP-4(2)	A1.3												
CP-5													
CP-6	A1.2	EC:SG4.SP1							164.308(a)(7)(ii)(B) 164.310(a)(2)(i)	11.1.4 & 17.1.2	9.3.6.5		
CP-6(1)	A1.2												
CP-6(2)	A1.2												
CP-6(3)	A1.2												
CP-7	A1.2	EC:SG4.SP1							164.308(a)(7)(ii)(B) 164.310(a)(2)(i)	11.1.4 & 17.1.2	9.3.6.6		
CP-7(1)	A1.2												
CP-7(2)	A1.2												
CP-7(3)	A1.2												
CP-7(4)	A1.2												
CP-7(6)	CC3.2 CC3.3												
CP-8	A1.2	EC:SG4.SP4							164.308(a)(7)(ii)(B)	11.2.2 & 17.1.2			
CP-8(1)	A1.2												
CP-8(2)	A1.2												
CP-8(3)	A1.2												
CP-8(4)	A1.2 A1.3 CC3.2 CC3.3												

WISP-LMH # NIST 800-53 Rev4	NISPOM	NIST CSF v1.1	NIST 800-171 rev 1	NIST 800-171B [initial draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2	Secure Controls Framework (SCF)	UK Cyber Essentials	Target Audience	Applicability
SA-2	8-100 8-200							PRM-03		Management	Basic
SA-3	8-311 8-610	PR.IP-2						PRM-07 SEA-07.1		Technical Users	Basic
SA-4	8-302 8-613	PR.IP-2 & DE.CM-6						TDA-02 TPM-01 TPM-10		Technical Users	Basic
SA-4(1)								TDA-04.1		Technical Users	Enhanced
SA-4(2)								TDA-04.1		Technical Users	Enhanced
SA-4(3)								TDA-02.3		Technical Users	Enhanced
SA-4(6)								TDA-03		Technical Users	Basic
SA-4(8)								TDA-09.1		Technical Users	Enhanced
SA-4(9)								TDA-02.1		Technical Users	Enhanced
SA-4(10)								TDA-02.2		Technical Users	Enhanced
SA-5	8-202 8-320 8-610	ID.RA-1			500.08			TDA-04		Technical Users	Basic
SA-6										N/A	N/A
SA-7										N/A	N/A
SA-8	8-311	PR.IP-2	3.13.1 3.13.2	3.14.3e	500.08		2.2	CFG-02 SEA-01		Technical Users	Basic
SA-9	8-700	ID.AM-4, PR.AT-3 & DE.CM-6				622(2)(d)(A)(v)		TPM-04		Technical Users	Basic
SA-9(1)						622(2)(d)(A)(v)	2.4, 12.8- 12.8.4	TPM-04.1		Technical Users	Basic
SA-9(2)								TPM-04.2		Technical Users	Basic
SA-9(3)							2.6 & 12.9	TPM-05		Management	Basic
SA-9(4)								TPM-04.3		Management	Enhanced
SA-9(5)								CLD-09 DCH-19 TPM-04.4		Management	Enhanced
SA-10	8-613	PR.IP-1, PR.IP-2 & PR.IP-3						TDA-14		Management	Basic
SA-10(1)								TDA-14.1		Technical Users	Enhanced
SA-11	8-302	ID.RA-1 & PR.IP-2					6.4 & 6.4.4	TDA-09		Technical Users	Basic
SA-11(1)							6.3, 6.3.1 & 6.3.2	TDA-09.2		Technical Users	Enhanced
SA-11(2)							6.6	TDA-15		Technical Users	Basic
SA-11(8)								TDA-09.3		Technical Users	Enhanced
SA-12		ID.BE-1 & PR.IP-2			500.11			TPM-03		Management	Basic
SA-12(1)								TPM-03.1		Management	Enhanced
SA-12(2)					500.11			TPM-08		Management	Enhanced
SA-12(5)								TPM-03.2		Management	Enhanced
SA-12(10)								TDA-11		Technical Users	Enhanced
SA-12(15)								TPM-03.3		Management	Enhanced
SA-13	8-302 8-311							SEA-01		Management	Enhanced
SA-14		ID.AM-5, ID.BE-3, ID.BE-4, ID.BE-5, ID.RA-4 & ID.RM-3			500.11			PRM-05 TPM-02		Management	Enhanced
SA-15		PR.IP-2					6.3, 6.5, 6.5.1-6.5.10	TDA-06		Technical Users	Basic
SA-15(9)							6.4 & 6.4.3	TDA-10		Technical Users	Basic
SA-16								TDA-16		Management	Basic
SA-17		PR.IP-2		3.14.1e				TDA-05		Technical Users	Basic
SA-18	8-308							AST-15		Technical Users	Enhanced
SA-18(2)							9.1, 9.1.1, 9.9 & 9.9.1-9.9.3	AST-15.1		Technical Users	Enhanced
SA-19	8-302							TDA-11		Management	Basic
SA-19(1)								TDA-11.1		Management	Enhanced
SA-19(3)								TDA-11.2		Technical Users	Basic
SA-20								TDA-12		Technical Users	Enhanced
SA-21				3.9.1e 3.9.2e				TDA-13		Management	Basic
SA-22	8-302							TDA-17		Technical Users	Basic
SA-22(1)								TDA-17.1		Technical Users	Basic
AT-1	8-101				500.14			SAT-01		Management	Basic
AT-2	8-101	PR.AT-1	3.2.1 3.2.2	3.2.1e	500.14		12.6	SAT-02		Management	Basic
AT-2(1)				3.2.2e				SAT-02.1		Management	Enhanced
AT-2(2)			3.2.3					THR-05		Management	Enhanced
AT-3	8-101 8-103 8-104	PR.AT-2, PR.AT-4 & PR.AT-5	3.2.1 3.2.2		500.10 500.14	622(2)(d)(A)(iv	1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 10.9, 11.6, 12.6, 12.6.1, 12.6.2, 12.8.3, 12.8.5 & 12.10.4	SAT-03		Management	Basic
AT-3(3)								SAT-03.1		Management	Enhanced
AT-3(4)								SAT-03.6		Management	Enhanced
AT-4	8-103 8-104				500.14		12.6.2	SAT-04		Management	Basic
AT-5							6.2 & 12.4			N/A	N/A
CP-1	8-603							BCD-01		Management	Basic
CP-2	8-614	ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-5, PR.DS-4, PR.IP-4, PR.IP-7, PR.IP-9, PR.IP-10, DE.AE-4, RS.AN-2, RS.AN-4, RS.CO-1, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3						BCD-01 BCD-06		Management	Basic
CP-2(1)								BCD-01.1		Management	Basic
CP-2(2)								CAP-03		Management	Enhanced
CP-2(3)								BCD-02.3		Management	Basic
CP-2(4)								BCD-02.1		Management	Enhanced
CP-2(5)								BCD-02.2		Management	Basic
CP-2(6)								BCD-01.3		Management	Enhanced
CP-2(8)								BCD-02		Management	Basic
CP-3	8-615	RS.CO-1						BCD-03		Management	Basic
CP-3(1)								BCD-03.1		Management	Enhanced
CP-4	8-615							BCD-04 BCD-05		Management	Basic
CP-4(1)								BCD-04.1		Management	Basic
CP-4(2)								BCD-04.2		Management	Enhanced
CP-5										N/A	N/A
CP-6	8-603	PR.IP-4						BCD-08		Management	Enhanced
CP-6(1)								BCD-08.1		Management	Enhanced
CP-6(2)								BCD-01.4		Management	Basic
CP-6(3)								BCD-08.2		Management	Enhanced
CP-7	8-603							BCD-09		Management	Enhanced
CP-7(1)								BCD-09.1		Management	Enhanced
CP-7(2)								BCD-09.2		Management	Enhanced
CP-7(3)								BCD-09.3		Management	Enhanced
CP-7(4)								BCD-09.4		Management	Enhanced
CP-7(6)								BCD-09.5		Management	Enhanced
CP-8	8-615	ID.BE-4 & PR.PT-4						BCD-10		Management	Basic
CP-8(1)								BCD-10.1		Management	Enhanced
CP-8(2)								BCD-10		Management	Enhanced
CP-8(3)								BCD-10.2		Management	Enhanced
CP-8(4)								BCD-10.3		Management	Enhanced

WISP-LM # NIST 800-53 Rev4	WISP-LMH # NIST 800-53 Rev4	Control Grouping	WISP - Standard Name	NIST 800-53 rev4 LOW	NIST 800-53 rev4 MODERATE	NIST 800-53 rev4 HIGH	NIST 800-53 rev4 No Category	FedRAMP LOW	FedRAMP MODERATE	FedRAMP HIGH	FedRAMP LI-SaaS
CP-9	CP-9	Operational	Information System Backup	x	x	x		x	x	x	x
CP-9(1)	CP-9(1)	Operational	Information System Backup | Testing for Reliability & Integrity		x	x			x	x	
Not Included	CP-9(2)	Operational	Information System Backup | Test Restoration Using Sampling			x				x	
CP-9(3)	CP-9(3)	Operational	Information System Backup | Separate Storage for Critical Information			x			x	x	
Not Included	CP-9(5)	Operational	Information System Backup | Transfer to Alternate Storage Site			x				x	
Not Included	CP-9(6)	Operational	Information System Backup | Redundant Secondary System				x				
Not Included	CP-9(7)	Operational	Information System Backup | Dual Authorization				x				
CP-10	CP-10	Operational	Information System Recovery & Reconstitution	x	x	x		x	x	x	x
CP-10(2)	CP-10(2)	Operational	Information System Recovery & Reconstitution | Transaction Recovery		x	x			x	x	
Not Included	CP-10(4)	Operational	Information System Recovery & Reconstitution | Restore Withing Time Period			x				x	
Not Included	CP-10(6)	Operational	Information System Recovery & Reconstitution | Component Protection				x				
CP-11	CP-11	Operational	Alternate Communications Protocols				x				
CP-12	CP-12	Operational	Safe Mode				x				
CP-13	CP-13	Operational	Alternative Security Mechanisms				x				
IR-1	IR-1	Operational	Incident Response Policy & Procedures	x	x	x		x	x	x	x
IR-2	IR-2	Operational	Incident Response Training	x	x	x		x	x	x	x
Not Included	IR-2(1)	Operational	Incident Response Training | Simulated Events			x				x	
Not Included	IR-2(2)	Operational	Incident Response Training | Automated Training Environments			x				x	
IR-3	IR-3	Operational	Incident Response Testing		x	x			x	x	
IR-3(2)	IR-3(2)	Operational	Incident Response Testing | Coordination with Related Plans		x	x			x	x	
IR-4	IR-4	Operational	Incident Handling	x	x	x		x	x	x	x
IR-4(1)	IR-4(1)	Operational	Incident Handling | Automated Incident Handling Processes		x	x			x	x	
Not Included	IR-4(2)	Operational	Incident Handling | Dynamic Reconfiguration				x			x	
Not Included	IR-4(3)	Operational	Incident Handling | Continuity of Operations				x			x	
Not Included	IR-4(4)	Operational	Incident Handling | Information Correlation			x				x	
Not Included	IR-4(6)	Operational	Incident Handling | Insider Threats - Specific Capabilities				x			x	
Not Included	IR-4(8)	Operational	Incident Handling | Correlation with External Organizations				x			x	
IR-5	IR-5	Operational	Incident Monitoring	x	x	x		x	x	x	x
Not Included	IR-5(1)	Operational	Incident Monitoring | Automated Tracking / Data Collection / Analysis			x				x	
IR-6	IR-6	Operational	Incident Reporting	x	x	x		x	x	x	x
IR-6(1)	IR-6(1)	Operational	Incident Reporting | Automated Reporting		x	x			x	x	
IR-7	IR-7	Operational	Incident Response Assistance	x	x	x		x	x	x	x
IR-7(1)	IR-7(1)	Operational	Incident Response Assistance | Automation Support of Availability of Information / Support		x	x			x	x	
IR-7(2)	IR-7(2)	Operational	Incident Response Assistance | Coordination With External Providers				x		x	x	
IR-8	IR-8	Operational	Incident Response Plan (IRP)	x	x	x		x	x	x	x
IR-9	IR-9	Operational	Information Spillage Response				x		x	x	x
IR-9(1)	IR-9(1)	Operational	Information Spillage Response | Responsible Personnel				x		x	x	
IR-9(2)	IR-9(2)	Operational	Information Spillage Response | Training				x		x	x	
IR-9(3)	IR-9(3)	Operational	Information Spillage Response | Post-Spill Operations				x		x	x	
IR-9(4)	IR-9(4)	Operational	Information Spillage Response | Exposure to Unauthorized Personnel				x		x	x	
IR-10	IR-10	Operational	Integrated Information Security Analysis Team				x				
MP-1	MP-1	Operational	Media Protection Policy & Procedures	x	x	x		x	x	x	x
MP-2	MP-2	Operational	Media Access	x	x	x		x	x	x	x
MP-3	MP-3	Operational	Media Marking		x	x			x	x	
MP-4	MP-4	Operational	Media Storage		x	x			x	x	
MP-5	MP-5	Operational	Media Transport		x	x			x	x	
Not Included	MP-5(3)	Operational	Media Transport | Custodians				x				
MP-5(4)	MP-5(4)	Operational	Media Transport | Cryptographic Protection (Encrypting Data In Storage Media)		x	x			x	x	
MP-6	MP-6	Operational	Media Sanitization	x	x	x		x	x	x	x
Not Included	MP-6(1)	Operational	Media Sanitization | Review, Approve, Track, Document & Verify			x				x	
MP-6(2)	MP-6(2)	Operational	Media Sanitization | Equipment Testing			x			x	x	
Not Included	MP-6(3)	Operational	Media Sanitization | Non-Destructive Techniques			x				x	
Not Included	MP-6(7)	Operational	Media Sanitization | Dual Authorization				x				
MP-7	MP-7	Operational	Media Use	x	x	x		x	x	x	x
MP-7(1)	MP-7(1)	Operational	Media Use | Prohibit Use Without Owner		x	x			x	x	
MP-8	MP-8	Operational	Media Downgrading				x				
PS-1	PS-1	Operational	Personnel Security Policy & Procedures	x	x	x		x	x	x	x
PS-2	PS-2	Operational	Position Risk Designation (Position Categorization)	x	x	x		x	x	x	x
PS-3	PS-3	Operational	Personnel Screening	x	x	x		x	x	x	x
PS-3(3)	PS-3(3)	Operational	Personnel Screening | Information With Special Protection Measures				x		x	x	
PS-4	PS-4	Operational	Personnel Termination	x	x	x		x	x	x	x
Not Included	PS-4(1)	Operational	Personnel Termination | Post-Employment Requirements				x				
Not Included	PS-4(2)	Operational	Personnel Termination | Automated Notification			x				x	
PS-5	PS-5	Operational	Personnel Transfer	x	x	x		x	x	x	x
PS-6	PS-6	Operational	Access Agreements	x	x	x		x	x	x	x
Not Included	PS-6(3)	Operational	Access Agreements | Post-Employment Requirements				x				
PS-7	PS-7	Operational	Third-Party Personnel Security	x	x	x		x	x	x	x
PS-8	PS-8	Operational	Personnel Sanctions	x	x	x		x	x	x	x
PE-1	PE-1	Operational	Physical and Environmental Protection Policy & Procedures	x	x	x		x	x	x	x
PE-2	PE-2	Operational	Physical Access Authorizations	x	x	x		x	x	x	x
Not Included	PE-2(1)	Operational	Physical Access Authorizations | Access by Position / Role				x				
Not Included	PE-2(2)	Operational	Physical Access Authorizations | Two Forms of Identification				x				
Not Included	PE-2(3)	Operational	Physical Access Authorizations | Restrict Unescorted Access				x				
PE-3	PE-3	Operational	Physical Access Control	x	x	x		x	x	x	x
Not Included	PE-3(1)	Operational	Physical Access Control | Information System Access			x				x	
Not Included	PE-3(4)	Operational	Physical Access Control | Lockable Casings				x				
PE-4	PE-4	Operational	Access Control for Transmission Medium		x	x			x	x	
PE-5	PE-5	Operational	Access Control for Output Devices		x	x			x	x	
PE-6	PE-6	Operational	Monitoring Physical Access	x	x	x		x	x	x	x
PE-6(1)	PE-6(1)	Operational	Monitoring Physical Access | Intusion Alarms / Surveillance Equipment		x	x			x	x	
Not Included	PE-6(4)	Operational	Monitoring Physical Access | Monitoring Physical Acces to Information Systems			x				x	
PE-7	PE-7	Withdrawn	Visitor Control [withdrawn into PE-2 and PE-3]								
PE-8	PE-8	Operational	Visitor Access Records	x	x	x		x	x	x	x

WISP-LMH # NIST 800-53 Rev4	AICPA TSC 2017 (SOC 2)	CERT RMM v1.2	CIS CSC v7.1	DoD CMMC 0.6	FACTA	FAR 52.204-21	Generally Accepted Privacy Principles (GAPP)	GLBA	HIPAA	ISO 27002 v2013	IRS 1075	MA 201 CMR 17.00
CP-9	A1.2 CC6.6	KIM:SG6.SP1	10.1 10.2 10.4	RE.2.137 RE.2.138 RE.3.139					164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.310(d)(2)(iv)	12.3.1, 17.1.2 & 18.1.3	9.3.6.7	
CP-9(1)	A1.3		10.3	RE.2.137								
CP-9(2)	A1.3											
CP-9(3)	A1.2		10.4									
CP-9(5)	A1.2			RE.3.139								
CP-9(6)	A1.2											
CP-9(7)	A1.2											
CP-10	CC3.2	SC:SG3.SP1	5.5						164.308(a)(7)(ii)(B)	17.1.2	9.3.6.8	
CP-10(2)	A1.2											
CP-10(4)	A1.2											
CP-10(6)	A1.2		10.4									
CP-11	A1.2									17.1.2		
CP-12	CC7.2	EC:SG2.SP2 KIM:SG2.SP2										
CP-13	CC6.1	EC:SG2.SP2 SC:SG1.SP1								17.1.2		
IR-1	CC5.1 CC5.2						1.2.7		164.308(a)(6)(i)	5.1.1, 5.1.2, 6.1.1, 12.1.1, 16.1.2, 16.1.1, 18.1.1 & 18.2.2	9.3.8.1	
IR-2	CC1.4	SC:SG3.SP5	19.7	IR.2.092					164.308(a)(5)(i)	7.2.2 & 12.2.1	9.3.8.2	
IR-2(1)	CC1.4											
IR-2(2)	CC1.4											
IR-3	CC7.3 CC7.4			IR.3.099					164.308(a)(6)(i)		9.3.8.3	
IR-3(2)	CC7.3 CC7.4						1.2.7					
IR-4	CC7.3 CC7.4 CC7.5	IMC:SG1.SP1 IMC:SG1.SP2 IMC:SG2.SP1 IMC:SG2.SP2 IMC:SG2.SP3 IMC:SG2.SP4 IMC:SG3.SP1 IMC:SG3.SP2 IMC:SG4.SP1 IMC:SG4.SP2 IMC:SG4.SP3 IMC:SG4.SP4 IMC:SG5.SP1		IR.2.092 IR.2.093 IR.2.094 IR.2.095 IR.3.098 IR.2.097			1.2.7		164.308(a)(6)(ii)	6.1.[illegible]16.1.4, 16.1.6 & 16.1.7	9.3.8.4	
IR-4(1)	CC7.3 CC7.4											
IR-4(2)	CC7.3 CC7.4											
IR-4(3)	CC7.3 CC7.4											
IR-4(4)	CC7.3 CC7.4		6.7 6.8									
IR-4(6)	CC7.3 CC7.4				x							
IR-4(8)	CC7.3 CC7.4											
IR-5	CC7.3 CC7.4	IMC:SG2.SP1 IMC:SG2.SP2		IR.2.092 IR.2.093			1.2.7		[illegible]308(a)(1)(ii)(D) 164.308(a)(6)(ii)		9.3.8.5	
IR-5(1)	CC7.3 CC7.4											
IR-6	CC7.2	IMC:SG2.SP1	19.4 19.5	IR.2.092 IR.2.093			[illegible]		164.308(a)(1)(ii)(D) 164.308(a)(6)(ii)	6.1.3 & 16.1.2	9.3.8.6	17.03(2)(j)
IR-6(1)	CC7.3 CC7.4											
IR-7	CC7.2	IMC:SG2.SP2	19.5	IR.2.092			1.2.7		164.308(a)(6)(ii)	6.1.3	9.3.8.7	
IR-7(1)	CC7.3 CC7.4									6.1.3		
IR-7(2)	CC7.3 CC7.4											
IR-8	CC7.3 CC7.4 CC7.5	IMC:SG1.SP1 IMC:SG1.SP2	19.1 19.2 19.3 19.8				1.2.8			12.2.1	9.3.8.8	
IR-9	CC7.3 CC7.4	IMC:SG4.SP1 IMC:SG4.SP2	19.5	IR.2.095							9.3.8.9	
IR-9(1)	CC7.3 CC7.4											
IR-9(2)	CC1.4											
IR-9(3)	A1.2											
IR-9(4)												
IR-10	CC7.3 CC7.4	IMC:SG1.SP2	19.3							16.1.6		
MP-1	CC5.1 CC5.2	KIM:SG2.SP2	13.1 14.4						164.310(d)(1)	5.1.1, 5.1.2, 6.1.1, 12.1.1, 8.3.1, 9.1.1, 11.2.9, 10.1.1, 18.1.1, 18.1.3 & 18.2.2	9.3.10.1	17.03(2)(c)
MP-2	CC6.4 CC6.5	AM:SG1.SP1 KIM:SG2.SP1 KIM:SG2.SP2		[illegible]119 [illegible]2.120		(b)(1)(vii)			164.308(a)(3)(ii)(A) 164.310(c) 164.310(d)(1)	8.1.2, 8.2.3, 8.3.1 & 11.2.9	9.3.10.2	
MP-3	CC6.7	KIM:SG4.SP2 KIM:SG4.SP3	13.1	[illegible]P.3.122			1.2.3		164.310(b) 164.310(c)	8.2.2 & 8.2.3	9.3.10.3	
MP-4	CC6.4 CC6.5	KIM:SG4.SP2		[illegible]		(b)(1)(vii)			164.310(c) 164.310(d)(1) 164.310(d)(2)(iv)	8.2.3, 8.3.1, 11.2.9 & 18.1.3	9.3.10.4	17.03(2)(c)
MP-5	CC6.7	[illegible] KIM:SG4.SP3		A[illegible].3.036 MP.3.124			8.2.6		164.310(d)(1) 164.310(d)(2)(iii)	8.2.3, 8.3.1, 8.3.3, 11.2.5 & 11.2.6	9.3.10.5	17.03(2)(c)
MP-5(3)	[illegible]											
MP-5(4)	[illegible]C6.7			MP.3.125								
MP-6	CC6.4 CC6.5	KIM:SG4.SP3		AM.3.036 MP.2.119 MP.2.120		(b)(1)(vii)			164.310(d)(1) 164.310(d)(2)(i) 164.310(d)(2)(ii)	8.2.3, 8.3.1, 8.3.2, 11.2.5, 11.2.6 & 11.2.7	9.3.10.6	
MP-6(1)	CC6.4											
MP-6(2)	CC6.4											
MP-6(3)	[illegible]											
MP-6(7)	[illegible]											
MP-7	[illegible]C6.6	KIM:S[illegible]	14.6	AM.3.036						8.2.3, 8.3.1 & 12.2.1		
MP-7(1)	[illegible]6.6			MP.3.123								
MP-8	[illegible]	[illegible]SG4.SP3										
PS-1	[illegible]								164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B)	5.1.1, 5.1.2, 6.1.1, 12.1.1, 16.1.2, 18.1.1 & 18.2.2	9.3.13.1	
PS-2	CC1.1		17.1						164.308(a)(3)(ii)(B)	6.1.1	9.3.13.2	
PS-3	CC1.1			PS.2.127 PS.2.128					164.308(a)(3)(ii)(B)	7.1.1	9.3.13.3	
PS-3(3)	CC1.1											
PS-4	A1.2 CC6.2 CC6.3			PS.2.127 PS.2.128					164.308(a)(3)(ii)(C)	7.3.1, 8.1.4 & 9.2.6	9.3.13.4	17.03(2)(e)
PS-4(1)												
PS-4(2)	CC6.2											
PS-5	CC6.3			PS.2.127					164.308(a)(3)(ii)(C)	7.3.1, 8.1.4 & 9.2.6	9.3.13.5	
PS-6	CC1.1								164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4)(ii)(B) 164.310(b) 164.310(d)(2)(iii) 164.314(a)(1) 164.314(a)(2)(i)	13.2.4, 15.1.2, 8.1.3, 6.1.1, 7.1.2, 7.2.1, 13.2.1, 6.2.1 & 6.2.2	9.3.13.6	
PS-6(3)												
PS-7	CC1.5 CC1.1 CC4.1 CC4.2 CC6.4								164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.308(b)(1) 164.314(a)(1) 164.314(a)(2)(i)	6.1.1, 15.1.2 & 7.2.1	9.3.13.7	
PS-8	CC1.3				X					7.2.3	9.3.13.8	17.03(2)(d)
PE-1	CC5.1 CC5.2	AM:SG1.SP1					8.2.3 8.2.4		164.310(a)(1) 164.310(a)(2)(ii)	5.1.1, 5.1.2, 6.1.1, 11.1.4, 11.1.5, 12.1.1, 18.1.1 & 18.1.2	9.3.11.1	
PE-2	CC6.4 CC6.5	AM:SG1.SP1 EC:SG2.SP2 HRM:SG2.SP1 ID:SG1.SP1 ID:SG1.SP2		PE.1.131 PE.2.135		(b)(1)(viii)			164.310(a)(1) 164.310(a)(2)(iii)	9.2.6 & 11.1.2	9.3.11.2	
PE-2(1)	CC6.4											
PE-2(2)	CC6.4											
PE-2(3)	CC6.4											
PE-3	CC6.4 CC6.5	AM:SG1.SP1 EC:SG2.SP1 EC:SG2.SP2		PE.1.132 PE.1.133 PE.1.134		(b)(1)(ix) (b)(1)(ix)			164.310(a)(1) 164.310(a)(2)(iii) 164.310(b)	11.1.1, 11.1.2, 11.1.3 & 11.1.6	9.3.11.3	17.03(2)(g)
PE-3(1)	CC6.4											
PE-3(4)	CC6.4											
PE-4	CC6.4	EC:SG2.SP1		PE.1.131		(b)(1)(viii)			164.310(a)(1)	11.1.1, 11.1.2, 11.1.3 & 11.2.3	9.3.11.4	
PE-5	CC6.4 CC6.5	KIM:SG2.SP2 TM:SG2.SP2		PE.1.131 PE.2.135		(b)(1)(viii)			164.310(a)(1) 164.310(b)	11.1.1, 11.1.2 & 11.1.3	9.3.11.5	
PE-6	CC6.4 CC6.5	EC:SG2.SP1 IMC:SG2.SP1		IR.2.093 PE.1.131		(b)(1)(viii)			164.310(a)(2)(iii)	11.1.2 & 12.4.1	9.3.11.6	
PE-6(1)	CC6.4											
PE-6(4)	CC6.4											
PE-7									164.310(a)(2)(iii)			
PE-8	CC6.4	ADM:SG1.SP1							164.310(a)(2)(iii)	11.1.2 & 12.4.1	9.3.11.7	

WISP-LMH # NIST 800-53 Rev4	NERC CIP	NISPOM	NIST CSF v1.1	NIST 800-171 rev 1	NIST 800-171B [initial draft]	NY DFS 23 NYCRR500	OR 646A	PCI DSS v3.2	Secure Controls Framework (SCF)	UK Cyber Essentials	Target Audience	Applicability
CP-9		8-603 8-612	PR.IP-4	3.8.9					BCD-11		Technical Users	Basic
CP-9(1)									BCD-11.1		Technical Users	Basic
CP-9(2)									BCD-11.5		Technical Users	Enhanced
CP-9(3)									BCD-11.2		Technical Users	Enhanced
CP-9(5)									BCD-11.6		Technical Users	Enhanced
CP-9(6)									BCD-11.7		Technical Users	Enhanced
CP-9(7)					3.1.1e				BCD-11.8		Technical Users	Enhanced
CP-10		8-613	RS.RP-1 & RC.RP-1						BCD-12		Technical Users	Basic
CP-10(2)									BCD-12.1		Technical Users	Enhanced
CP-10(4)									BCD-12.4		Technical Users	Enhanced
CP-10(6)									BCD-13		Technical Users	Enhanced
CP-11		8-601 8-603	ID.BE-5						BCD-10		Technical Users	Enhanced
CP-12		8-615							SEA-07.2		Technical Users	Enhanced
CP-13		8-605 8-607							BCD-07		Technical Users	Enhanced
IR-1		8-101 8-103				500.16			IRO-01 IRO-04.2		Management	Basic
IR-2		8-103		3.6.1					IRO-05		Management	Basic
IR-2(1)									IRO-05.1		Management	Enhanced
IR-2(2)									IRO-05.2		Management	Enhanced
IR-3		8-104	PR.IP-10 & RS.CO-1	3.6.3					IRO-06		Management	Basic
IR-3(2)									IRO-06.1		Management	Basic
IR-4		1-303 4-218	DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.CO-3, RS.CO-4, RS.IM 1, RS.IM-2, RS.MI-1, RS.MI-2, RS.RP-1, RC.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3	3.6.1 3.6.2		500.16		12.5.3	IRO-02		Management	Basic
IR-4(1)									IRO-02.1		Management	Enhanced
IR-4(2)									IRO-02.3		Management	Enhanced
IR-4(3)									BCD-01 IRO-02.4		Management	Enhanced
IR-4(4)									MON-02.1		Management	Enhanced
IR-4(6)									IRO-02.2		Management	Enhanced
IR-4(8)									IRO-02.5		Management	Enhanced
IR-5		1-303 4-218	DE.AE-3, DE.AE-5, RS.AN-1 & RS.AN-4	3.6.1 3.6.2				12.5.2	IRO-09		Management	Basic
IR-5(1)									IRO-09.1		Management	Enhanced
IR-6		1-303 4-218	RS.CO-2	3.6.1 3.6.2		500.16 500.17	604(1)-(5)	12.8.3	GOV-06 IRO-10		All Users	Basic
IR-6(1)									IRO-10.1		Management	Enhanced
IR-7				3.6.1	3.6.2e	500.17			IRO-11		Management	Basic
IR-7(1)									IRO-11.1		Management	Enhanced
IR-7(2)			RS.CO-1, RS.CO-4, RC.CO-1, RS.CO-2 & RS.CO-3			500.16			IRO-11.2		Management	Enhanced
IR-8		8-103 1-302	PR.IP-7, PR.IP-9, DE.AE-3, DE.AE-5, RS.AN-4, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.RP-1, RC.IM-1 &			500.16	622(2)(d)(B)(iii)	12.8.3, 12.10, 12.10.1-12.10.6	IRO-04		Management	Basic
IR-9		8-103							IRO-12		Management	Basic
IR-9(1)									IRO-12.1		Management	Enhanced
IR-9(2)									IRO-12.2		Management	Enhanced
IR-9(3)									IRO-12.3		Management	Enhanced
IR-9(4)									IRO-12.4		Management	Enhanced
IR-10						500.16		12.10.3	IRO-07		Management	Basic
MP-1		8-306 8-309							DCH-01		Management	Basic
MP-2		8-310	PR.PT-2	3.8.1 3.8.2 3.8.3					DCH-03 END-01		Technical Users	Basic
MP-3		8-306 8-310		3.8.4					DCH-04		All Users	Basic
MP-4		8-308	PR.PT-2	3.8.1 3.8.2 3.8.3			622(2)(d)(C)(i) & 620	9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.7, 9.7.1 & 9.9	DCH-06		All Users	Basic
MP-5		8-605	PR.PT-2	3.8.5			620	9.6, 9.6.2, 9.6.3 & 9.7	DCH-07		All Users	Basic
MP-5(3)									DCH-07.1		All Users	Basic
MP-5(4)				3.8.6		500.15			DCH-07.2		All Users	Basic
MP-6		8-301 8-608	PR.DS-3 & PR.IP-6	3.8.1 3.8.2 3.8.3			622(2)(d)(C)(i) & 622(2)(d)(C)(iv)	9.8, 9.8.1 & 9.8.2	DCH-08 DCH-09		All Users	Basic
MP-6(1)								9.7.1	DCH-09.1		Technical Users	Basic
MP-6(2)									DCH-09.2		Technical Users	Enhanced
MP-6(3)									DCH-09		Technical Users	Enhanced
MP-6(7)					3.1.1e				DCH-09.5		Technical Users	Enhanced
MP-7		8-306	PR.PT-2	3.8.7					DCH-10		Technical Users	Basic
MP-7(1)				3.8.8					DCH-10.2		Technical Users	Enhanced
MP-8		8-310							DCH-11		Technical Users	Enhanced
PS-1		8-307	PR.IP-11						HRS-01		Management	Basic
PS-2		8-307	PR.IP-11			500.10			HRS-02		Management	Basic
PS-3		8-103 8-104	PR.DS-5 & PR.IP-11	3.9.1 3.9.2	3.9.1e 3.9.2e			12.7	HRS-04		Management	Basic
PS-3(3)									HRS-04.1		Management	Enhanced
PS-4		8-303 5-309	PR.IP-11	3.9.1 3.9.2				9.3	HRS-09		Management	Basic
PS-4(1)									HRS-09.3		Management	Basic
PS-4(2)									HRS-09.4		Management	Enhanced
PS-5		8-303	PR.IP-11	3.9.1					HRS-08		Management	Basic
PS-6		8-103 8-104 8-105	PR.DS-5 & PR.IP-11						HRS-06 HRS-06.1		Management	Basic
PS-6(3)									HRS-06.2		Management	Basic
PS-7		8-304	ID.AM-6, ID.GV-2, PR.AT-3 & PR.IP-11						HRS-10		Management	Basic
PS-8		1-304	PR.IP-11						HRS-07		Management	Basic
PE-1		8-308							PES-01		Management	Basic
PE-2		8-308 5-306 5-308 6-104	PR.AC-2	3.10.1 3.10.2				9.2	PES-02		Management	Basic
PE-2(1)									PES-02.1		Management	Basic
PE-2(2)								9.4 & 9.4.1	PES-06.2		Management	Basic
PE-2(3)								9.3	PES-06.3		Management	Basic
PE-3		5-300 6-104	PR.AC-2, DE.CM-2, DE.CM-7 & DE.DP-3	3.10.3 3.10.4 3.10.5			622(2)(d)(C)(ii)	9.1, 9.1.1, 9.1.2, 9.2, 9.4.2 & 9.4.3	PES-03		Management	Basic
PE-3(1)									PES-03.4		Management	Basic
PE-3(4)									PES-03.2		Technical Users	Enhanced
PE-4		8-605	PR.AC-2	3.10.2			622(2)(d)(C)(ii)	9.1.2 & 9.1.3	PES-12.1		Technical Users	Basic
PE-5		8-310	PR.AC-2	3.10.1 3.10.2			622(2)(d)(C)(ii)		PES-12.2		All Users	Basic
PE-6		5-300	PR.AC-2, DE.CM-2, DE.CM-7, RS.AN-1 & RS.CO-3	3.10.1 3.10.2			622(2)(d)(C)(ii)	9.1 & 9.1.1	PES-05		Management	Basic
PE-6(1)									PES-05.1		Management	Enhanced
PE-6(4)									PES-05.2		Management	Enhanced
PE-7											N/A	N/A
PE-8							622(2)(d)(C)(ii)	9.4.4	PES-03.3		Management	Basic

EXAMPLE