WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
1	Information Security Program Policy												
1.2	Management Direction for Information Security	5.1								1.2.8			
1.2.1.1	Publishing An Information Security Policy	5.1.1			500.03					1.1.0 2.1.0-2.2.3 3.1.0-3.1.2 4.1.0-4.2.4 5.1.0-5.1.1 6.1.0-6.1.1 7.1.0-7.1.2 8.1.0-8.2.1 9.1.0-9.1.1 10.1.0-10.1.1			
1.2.1.2	Information Security Program Plan		12.1 & 12.1.1		500.02	164.308(a)(1)(i) & 164.316(a)-(b)	6801(b)(1)	17.03(1), 17.04 & 17.03(2)(b)(2)					ID.GV-1 & ID.GV-2
1.2.1.3	Assigned Information Security Responsibilities		12.5-12.5.5		500.04	164.308(a)(2)	Safeguards Rule	17.03(2)(a)	622(2)(d)(A)(i)				ID.AM-6 & ID.GV-2
1.2.1.4	Information Security Resources												
1.2.1.5	Risk Management		12.2		500.09								
1.2.2	Review of Information Security Policies	5.1.2								1.2.1			
1.2.2.1	Information Security Documentation Review				500.03								
2	Information Security Organization Policy												
2.1	Internal Organization	6.1								1.2.8			
2.1.1	Information Security Roles & Responsibilities	6.1.1								1.1.2			
2.1.1.1	Roles & Responsibilities				500.04								
2.1.1.2	Position Categorization				500.04	164.308(a)(3)(i) & (ii) & (A)							PR.IP-11
2.1.2	Segregation of Duties	6.1.2											
2.1.2.1	Incompatible Roles												
2.1.2.2	Two-Person Rule												
2.1.3	External Authorities	6.1.3											
2.1.3.1	Contacts With Authorities	6.1.3											
2.1.4	Special Interest Groups	6.1.4											
2.1.4.1	Contacts With Security Groups & Associations		5.1.2 & 6.1		500.10	164.308(A)(5)(ii) & (ii)(A)							ID.RA-2 & RS.CO-5
2.1.4.2	Security Industry Alerts & Notification Process		6.2 & 12.4			164.308(A)(5)(ii) & (ii)(A)							
2.1.5	Information Security in Project Management	6.1.5											
2.1.5.1	Security Assessments							17.03(2)(h)	622(2)(B)(i)-(iv)				ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3
2.1.5.2	System Security Plan (SSP)												PR.IP-7 & DE.DP-5
2.2	Mobile Devices and Teleworking	6.2											
2.2.1	Mobile Device Management	6.2.1											
2.2.1.1	Access Control For Mobile Devices	6.2.1											PR.AC-3
2.2.1.2	Central Management Of Mobile Devices												
2.2.1.3	Remote Purging												
2.2.1.4	Personally Owned Devices												
2.2.1.5	Tamper Protection & Detection												
2.2.2	Teleworking	6.2.2											
2.2.2.1	Telecommuting												
2.2.2.2	Remote Access	6.2.2	12.3.8 & 12.3.9										PR.AC-3 & PR.PT-4
2.2.2.3	Privileged Commands & Access												
2.2.2.4	Non-Local Maintenance												PR.MA-2
2.2.2.5	Non-Local Maintenance Approvals & Notifications												
2.2.2.6	Non-Local Maintenance Cryptographic Protection		2.3										
2.2.2.7	Remote Disconnect Verification												
2.2.2.8	Auditing												
3	Human Resource Security Policy												
3.1	Prior to Employment	7.1											
3.1.1	Screening	7.1.1								1.2.9			
3.1.1.1	Personnel Screening		12.7			164.308(a)(3)(ii) & (B)							PR.DS-5 & PR.IP-11
3.1.2	Terrms and Conditions of Employment	7.1.2											
3.1.2.1	Access Agreements					164.308(a)(4)(i)							PR.DS-5 & PR.IP-11
3.2	During Employment	7.2											
3.2.1	Management Responsibilities	7.2.1											
3.2.1.1	Rules of Behavior		4.2, 12.3, 12.3.1, 12.3.2, 12.3.5-.6, 12.3.10 &12.4			164.310(b)		17.03(2)(b)(2)					
3.2.1.2	Social Media & Social Networking Restrictions												
3.2.1.3	Position Categorization					164.308(a)(3)(i) & (ii) & (A)							PR.IP-11
3.2.1.4	Third-Party Personnel Security												ID.AM-6, ID.GV-2, PR.AT-3 & PR.IP-11
3.2.2	Information Security Awareness, Education and Training	7.2.2								1.1.1 1.2.10			
3.2.2.1	Information Security Workforce												PR.AT-1, PR.AT-2, PR.AT-4 & PR.AT-5
3.2.2.2	Security Training		12.6.1 & 12.6.2		500.14			17.04(8)	622(2)(d)(A)(iv)				PR.AT-2, PR.AT-4 & PR.AT-5

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
3.2.2.3	Awareness Training for Sensitive Information		1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.9, 11.6, 12.6, 12.6.1, 12.6.2, 12.8.3 & 12.8.5, 12.10.4		500.14								
3.2.2.4	Vendor Security Training												
3.2.2.5	Security Training Records		12.6.2										
3.2.2.6	Security Awareness		12.6			164.308(a)(5)(i) & 164.308(a)(5)(ii)(A)		17.04(8) & 17.03(2)(b)(1)					PR.AT-1
3.2.2.7	Testing, Training & Monitoring												PR.IP-10, DE.DP-1, DE.DP-2, DE.DP-3 & DE.DP-5
3.2.2.8	Practical Exercises												
3.2.2.9	Insider Threat Awareness												
3.2.2.10	Security Industry Alerts & Notification Process		6.2 & 12.4			164.308(A)(5)(ii) & (ii)(A)							
3.2.3	Disciplinary Process	7.2.3											
3.2.3.1	Personnel Sanctions					164.308(a)(1)(ii)(C)		17.03(2)(d)					PR.IP-11
3.2.3.2	Workplace Investigations												
3.3	Termination and Change of Employment	7.3											
3.3.1	Termination or Change of Employment Responsibilities												
3.3.1.1	Personnel Termination	7.3.1	9.3			164.308(a)(3)(ii) & (C)		MA201CMR17 17.03(2)(e)					PR.IP-11
3.3.1.2	High-Risk Terminations												
3.3.1.3	Personnel Transfer												PR.IP-11
4	Asset Management Policy												
4.1	Responsibility for Assets	8.1											
4.1.1	Inventory of Assets												
4.1.1.1	Information System Inventory	8.1.1											
4.1.1.2	Information System Component Inventory		2.4										
4.1.1.3	Approved Deviations		1.1.2			164.310(d)(2)(iii)							ID.AM-1, ID.AM-2, PR.DS-3, PR.PT-3 & DE.CM-7
4.1.1.4	Network Diagrams		1.1.2 & 1.1.3										
4.1.2	Ownership of Assets	8.1.2											
4.1.2.1	Default Settings		2.5									1-1	
4.1.2.2	Share Hosting Providers		2.6 & 12.8.1										
4.1.2.3	Intranets												ID.AM-4 & PR.AC-3
4.1.3	Acceptable Use of Assets	8.1.3											
4.1.3.1	Rules of Behavior		4.2, 12.3, 12.3.1, 12.3.2, 12.3.5-.6, 12.3.10 &12.4			164.310(b)		17.03(2)(b)(2)					
4.1.3.2	Social Media & Social Networking Restrictions												
4.1.3.3	Acceptable Use for Critical Technologies		12.3-12.3.10										
4.1.4	Return of Assets	8.1.4											
4.1.4.1	Asset Collection												
4.2	Information Classification	8.2								1.2.3			
4.2.1	Classification of Information	8.2.1								1.2.3			
4.2.1.1	Security Categorization		9.6.1										ID.AM-5, ID.RA-4 & ID.RA-5
4.2.2	Labeling of Information	8.2.2											
4.2.2.1	Media Marking												
4.2.3	Handling of Assets	8.2.3											
4.2.3.1	Media Transportation		9.6, 9.6.2, 9.6.3 & 9.7			164.310(d)(1)		17.03(2)(c)	620				PR.PT-2
4.2.3.2	Media Custodians												
4.2.3.3	Cryptographic Protection (Encrypting Data In Storage Media)				500.15								
4.3	Media Handling	8.3								7.1.2 7.2.1-7.2.2			
4.3.1	Management of Removable Media	8.3.1								8.2.6			
4.3.1.1	Media Use												PR.PT-2
4.3.1.2	Media Access					164.308(a)(4)(ii)(C)							PR.PT-2
4.3.2	Disposal of Media	8.3.2		7						5.2.1-5.2.3			
4.3.2.1	Data Retention & Disposal			7	500.13						Chapter29-Schedule1-Part1-Principle 5		
4.3.2.2	Media Sanitization		9.8, 9.8.1 & 9.8.2	7	500.13	164.310(d)(2)(i)			622(2)(d)(C)(i) & 622(2)(d)(C)(iv)				PR.DS-3 & PR.IP-6
4.3.2.3	Media Sanitization Documentation		9.7.1	7		164.310(d)(2)(ii)							
4.3.3	Physical Media Transfer	8.3.3								8.2.5			
4.3.3.1	Strict Control of Media		9.7-9.7.1										
5	Accesss Control Policy												
5.1	Business Requirements of Access Control	9.1								8.2.2			
5.1.1	Access Control	9.1.1		1, 5						8.2.2		2-1 3-1	
5.1.1.1	Identification & Authentication		8.1		500.07							2-1	
5.1.1.2	Access To Sensitive Data		7.1-7.1.4										
5.1.1.3	Access Control Procedures		8.1 & 8.4			164.312(a)(1)							
5.1.2	Access to Networks and Network Services	9.1.2		2									
5.1.2.1	Least Functionality		1.1.5, 1.2.1, 2.2.2, 2.2.4 & 2.2.5					17.03(2)(a)				2-1	PR.IP-1
5.1.2.2	Prevent Program Execution												
5.2	User Access Management	9.2		1								3-7	
5.2.1	User Registration and De-Registration	9.2.1											

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
5.2.1.1	User ID Management		8.1, 8.1.1-8.1.8									3-6	
5.2.1.2	Account Management		8.1.3-8.1.5, 8.2.2, 8.5, 8.5.1, 8.6 & 8.7			164.312(d)		17.04(1(a)				3-1	Framework PR.AC-1, PR.AC-4, DE.CM-1 & DE.CM-3
5.2.2	User Access Provisioning	9.2.2		1								3-1	
5.2.2.1	Account Provisioning		8.2-8.2.6									3-1	
5.2.2.2	Role-Based Access Control (RBAC)		7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3			164.308(a)(4(ii)(A) & (B) & (C)						3-1	
5.2.3	Management of Privileged Access Rights	9.2.3		1								3-2	
5.2.3.1	Privileged Commands & Access											3-2 3-3 3-4 3-5	
5.2.4	Management of Secret Authentication Information of Users	9.2.4											
5.2.4.1	User Identification & Authentication for Organizational Users		8.1.1 & 8.2			17.04(1)(c) & 17.04(2)(b)							
5.2.4.2	Multifactor Authentication		8.3-8.3.2	6	500.12								
5.2.4.3	Identifier Management (User Names)			6		164.312(a)(2)(i)		17.04(1)(d)					
5.2.4.4	Privileged Account Management			6									
5.2.4.5	Identification & Authentication (Non-Organizational Users)			6									
5.2.4.6	Service Provider Identification & Authentication (Vendors)			6									
5.2.5	Review of User Access Rights	9.2.5											
5.2.5.1	Periodic Review												
5.2.6	Removal or Adjustment of Access Rights	9.2.6		1									
5.2.6.1	Access Enforcement		7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3			164.308(a)(4(i) & (ii)		17.04(1)(b) & 17.04(2)(a)	622(2)(d)(C)(iii)				PR.AM-3, PR.AC-4 & PR.PT-3
5.3	Responsibilities	9.3											
5.3.1	Use of Secret Authentication Information	9.3.1											
5.3.1.1	Individual Credentials		8.6										
5.3.1.2	Credential Sharing		8.5-8.5.1										
5.4	System and Application Access Control	9.4		5									
5.4.1	Information Access Restriction	9.4.1		2									
5.4.1.1	Access Control Lists (ACLs)		7.2-7.2.3										
5.4.1.2	Database Access		8.7										
5.4.2	Secure Log-On Procedures	9.4.2		6									
5.4.2.1	Trusted Communications Path												
5.4.2.2	Device-To-Device Identification & Authentication												
5.4.2.3	System Use Notification (Logon Banners)												
5.4.2.3.1	System Use Notification | Standardized Microsoft Windows Logon Banner												
5.4.2.3.2	System Use Notification | Truncated Logon Banner												
5.4.2.4	Previous Logon Notification												
5.4.3	Password Management System	9.4.3		1									
5.4.3.1	Authenticator Management (Passwords)		8.1.2, 8.2.3, 8.2.4 & 8.2.5			164.308(a)(S)(ii)(D)		17.04(1)(b)-(e) & 17.04(2)(b)					
5.4.3.2	Vendor-Supplied Defaults		2.1, 2.1.1 & 8.3									2-1 2-2	
5.4.3.3	Authenticator Feedback												
5.4.3.4	Cryptographic Module Authentication		8.2.1										
5.4.3.5	Re-Authentication		8.1.8										
5.4.4	Use of Privileged Utility Programs	9.4.4		2									
5.4.4.1	Access Enforcement		7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3			164.308(a)(4(i) & (ii)		17.04(1)(b) & 17.04(2)(a)	622(2)(d)(C)(iii)				PR.AM-3, PR.AC-4 & PR.PT-3
5.4.4.2	Least Privilege								622(2)(d)(C)(iii)				PR.AC-4 & PR.DS-5
5.4.5	Access Control to Program Source Code	9.4.5											
5.4.5.1	Source Code												
5.4.5.2	Library Privileges												
6	Cryptography Policy												
6.1	Cyrptographic Controls	10.1											
6.1.1	Use of Cryptographic Controls	10.1.1			500.15								
6.1.1.1	Use of Cryptography		2.2.3 & 4.1		500.15	164.312(e)(2)(ii)							PR.DS-5
6.1.1.2	Transmission Confidentiality					164.312(e)(1) & 164.312(e)(2)(i)		17.04(3)	622(2)(d)(C)(iii)				
6.1.1.3	Non-Local Maintenance Cryptographic Protection		2.3										
6.1.1.4	Wireless Access Authentication & Encryption		4.1.1		500.15								
6.1.1.5	Encrypting Data At Rest		3.4 & 3.4.1		500.15	164.312(a)(2)(iv)		17.04(5)	622(2)(d)(C)(iii)				PR.DS-1
6.1.1.6	Non-Console Administrative Access		2.3										
6.1.2	Key management	10.1.2											
6.1.2.1	Key Management Program		3.5-3.5.5										
6.1.2.2	Key Management Processes		3.6-3.6.8										
7	Physical and Environmental Security Policy												
7.1	Secure Areas	11.1		8						8.2.3			
7.1.1	Physical Security Perimeter	11.1.1		8						8.2.3			
7.1.1.1	Physical Access Authorizations		9.2	8		164.310(a)(2)(ii)							PR.AC-2
7.1.1.2	Role-Based Physical Access			8		164.310(a)(2)(iii)							
7.1.1.3	Identification Requirement		9.4 & 9.4.1	9									
7.1.1.4	Restrict Unescorted Access		9.3	9									
7.1.1.5	Physical Access Control		9.1, 9.1.1, 9.1.2 & 9.2	8		164.310(a)(2)(iv)		17.03(2)(g)	622(2)(d)(C)(ii)				PR.AC-2, DE.CM-2, DE.CM-7 & DE.DP-3
7.1.1.6	Physical Access Logs			9									
7.1.1.7	Lockable Physical Casings												
7.1.1.8	Access Control For Transmission Medium		9.1.2 & 9.1.3						622(2)(d)(C)(ii)				PR.AC-2

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
7.1.1.9	Access Control For Output Devices								622(2)(d)(C)(ii)				PR.AC-2
7.1.1.10	Monitoring Physical Access		9.1 & 9.1.1			164.310(c)			622(2)(d)(C)(ii)				PR.AC-2, DE.CM-2, DE.CM-7, RS.AN-1 & RS.CO-3
7.1.1.11	Visitor Control		9.4.2 & 9.4.3						622(2)(d)(C)(ii)				
7.1.1.12	Access Records		9.4.4						622(2)(d)(C)(ii)				
7.1.2	Physical Entry Controls	11.1.2								8.2.3			
7.1.2.1	Facility Entry Controls		9.1-9.1.3										
7.1.2.2	Authorizing & Monitoring Visitors		9.4-9.4.4										
7.1.2.3	Distinguish Visitors from On-Site Personnel		9.2										
7.1.3	Securing Offices, Rooms and Facilities	11.1.3								8.2.3			
7.1.3.1	Physical Access Controls to Sensitive Areas		9.3										
7.1.3.2	Physically Secure All Media		9.5-9.5.1										
7.1.4	Protecting Against External and Environmental Threats	11.1.4								1.2.4 8.2.4			
7.1.4.1	Risk Assessment		12.2			164.308(a)(1)(ii)(A) & (B)	Safeguards Rule	17.03(2)(b)	622(2)(A)(ii)				ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, PR.IP-12, DE.AE-4 & RS.MI-3
7.1.4.2	Risk Ranking												
7.1.4.3	Security Industry Alerts & Notification Process		6.2 & 12.4			164.308(A)(5)(ii) & (ii)(A)							
7.1.4.4	Threat Analysis & Flaw Remediation		6.6										
7.1.5	Working in Secure Areas	11.1.5											
7.1.5.1	Workstation Security												
7.1.6	Delivery and Loading Areas	11.1.6											
7.1.6.1	Delivery & Removal								622(2)(d)(C)(ii)				PR.DS-3
7.2	Equipment	11.2											
7.2.1	Equipment Siting and Protection	11.2.1											
7.2.1.1	Location of Information System Components												PR.IP-5
7.2.1.2	Media Storage		9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.7 & 9.9			164.310(d)(2)(iv)		17.03(2)(c)	620 & 622(2)(d)(C)(i)				PR.PT-2
7.2.2	Supporting utilities	11.2.2											
7.2.2.1	Automatic Voltage Controls												
7.2.2.2	Emergency Shutoff												PR.IP-5
7.2.2.3	Emergency Power												ID.BE-4
7.2.2.4	Emergency Lighting												
7.2.2.5	Fire Protection												PR.IP-5
7.2.2.6	Fire Detection Devices												PR.IP-5
7.2.2.7	Fire Suppression Devices												
7.2.2.8	Temperature & Humidity Controls												PR.IP-5
7.2.2.9	Water Damage Protection												PR.IP-5
7.2.3	Cabling Security	11.2.3											
7.2.3.1	Power Equipment & Power Cabling												ID.BE-4 & PR.AC-2
7.2.4	Equipment Maintenance	11.2.4											
7.2.4.1	Controlled Maintenance												PR.MA-1
7.2.4.2	Maintenance Activities												
7.2.4.3	Maintenance Tools												PR.MA-1
7.2.4.4	Maintenance Personnel												PR.MA-1
7.2.4.5	Timely Maintenance												
7.2.5	Removal of Assets	11.2.5											
7.2.5.1	Delivery & Removal								622(2)(d)(C)(ii)				PR.DS-3
7.2.6	Security of Equipment and Assets Off-Premises	11.2.6											
7.2.6.1	Media Distribution		9.6-9.6.3										
7.2.7	Secure Disposal or Re-Use of Equipment	11.2.7											
7.2.7.1	Media Destruction		9.8-9.8.2										
7.2.8	Unattended User Equipment	11.2.8											
7.2.8.1	Device Storage in Automobiles												
7.2.8.2	Kiosks & Point of Sale Devices		9.9-9.9.3										
7.2.9	Clear Desks and Clear Screens	11.2.9											
7.2.9.1	Workplace Security												
8	Operations Security Policy												
8.1	Operational Procedures and Responsibilities	12.1								1.2.6			
8.1.1	Doccumented Operating Procedures	12.1.1								1.2.6			
8.1.1.1	Security Concept of Operations (CONOPS)												
8.1.1.2	Operational Security (OPSEC)												
8.1.1.3	System Security Plans												PR.IP-7 & DE.DP-5
8.1.2	Change Management	12.1.2								1.2.6			
8.1.2.1	Configuration Change Control												PR.IP-1, PR.IP-3, DE.CM-1 & DE.CM-7
8.1.2.2	Prohibition of Changes												
8.1.2.3	Security Representative for Changes												
8.1.2.4	Security Impact Analysis for Changes		6.4, 6.4.5, 6.4.5.1-6.4.5.4										PR.IP-1 & PR.IP-3
8.1.2.5	Configuration Management											2-2 2-3 2-4	
8.1.2.6	Baseline Configurations		1.1.1										PR.DS-7, PR.IP-1 & DE.AE-1
8.1.2.7	Baseline Configuration Reviews & Updates												
8.1.2.8	Retention of Previous Configurations												
8.1.2.9	Network Device Configuration File Synchronization		1.2.2										

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
8.1.3	Capacity Management	12.1.3											
8.1.3.1	Capacity Management												PR.DS-4 & PR.PT-1
8.1.4	Separation of Development, Testing and Operational Environments	12.1.4											
8.1.4.1	Separate Development & Test Environments		6.4.1										
8.2	Protection from Malware	12.2		13								4-1 4-2 4-3 4-4 4-5	
8.2.1	Controls Against Malware	12.2.1		13, 15									
8.2.1.1	Antimalware Mechanisms		5.3	13								4-1	
8.2.1.2	Antimalware Installation		5.1-5.1.2	13									
8.2.1.3	Antimalware Signature Updates		5.2	14								4-2	
8.2.1.4	Malware Protection Procedures		5.4	13									
8.3	Backup	12.3											
8.3.1	Information Backup	12.3.1											
8.3.1.1	Information System Backup					164.308(a)(7)(ii)(A)							PR.IP-4
8.3.1.2	Information System Recovery & Reconstitution					164.308(a)(7)(ii)(B)							RS.RP-1 & RC.RP-1
8.3.1.3	Transaction Recovery												
8.3.1.4	Failover Capability												
8.3.1.5	Electronic Discovery (eDiscovery)												
8.3.1.6	Information System Imaging												
8.3.1.7	Backup & Restoration Hardware Protection												
8.4	Logging and Monitoring	12.4		10									
8.4.1	Event Logging	12.4.1											
8.4.1.1	Automated Audit Trails		10.2-10.2.7		500.06								
8.4.1.2	Audit Trail Content		10.3-10.3.6		500.06								
8.4.1.3	Log Review		10.6-10.6.3 & 10.8-10.8.1		500.06								
8.4.1.4	Linking Access to Individual Users		10.1		500.06								
8.4.2	File Integrity Monitoring (FIM)		11.5-11.5.1										
8.4.3	Protection of Log Information	12.4.2											
8.4.3.1	Securing Audit Trails		10.5-10.5.5										
8.4.3.2	Retention of Audit Trail History		10.7										
8.4.4	Administrator and Operator Logs	12.4.3											
8.4.4.1	Privileged Functions Logging		10.2 & 10.2.1-10.2.7										
8.4.5	Clock Synchronization	12.4.4											
8.4.5.1	Network Time Protocol (NTP)		10.4-10.4.3										
8.5	Control of Operational Software	12.5											
8.5.1	Installation of Software on Operational Systems	12.5.1											
8.5.1.1	Access Restriction for Change												PR.IP-1
8.6	Technical Vulnerability Management	12.6											
8.6.1	Management of Technical Vulnerabilities	12.6.1											
8.6.1.1	Software Patching		6.2									5-1 5-2 5-3 5-4	
8.6.1.2	Vulnerability Scanning		11.2-11.2.3	15	500.05							5-4	
8.6.1.3	Penetration Testing		11.3-11.3.4.1		500.05								
8.6.1.4	Vulnerability Ranking		6.1										
8.6.1.5	Vulnerability Remediation		6.6										
8.6.2	Restrictions on Software Installation	12.6.2											
8.6.2.1	User-Installed Software												DE.CM-3
8.6.2.2	Unauthorized Installation Alerts												
8.6.2.3	Prohibit Installation Without Privileged Status												
8.7	Information Systems Audit Considerations	12.7											
8.7.1	Information Systems Audit Controls	12.7.1											
8.7.1.1	Security-Related Activity Planning							17.03(2)(b)(i)					
9	Communications Security Policy												
9.1	Network Security Management	13.1										1-5	
9.1.1	Network Controls	13.1.1		3									
9.1.1.1	Firewall & Router Configurations		1.1-1.1.7									1-2 1-3 1-4	
9.1.1.2	Safeguarding Data over Open Networks		4.1-4.1.1										
9.1.1.3	Transmitting Sensitive Data		4.2										
9.1.1.4	Rogue Wireless Detection		11.1-11.1.2										
9.1.1.5	Intrusion Detection & Prevention Systems		11.4										
9.1.2	Security of Network Services	13.1.2		3									
9.1.2.1	Restricting Connections		1.2-1.2.3										
9.1.3	Segregation in Networks	13.1.3		3, 11									
9.1.3.1	Security Function Isolation		1.2, 1.3.1, 2.2.1 & 11.3.4										
9.1.3.2	Layered Defenses		1.3.7										
9.1.3.3	Application Partitioning		11.3.4										
9.2	Information Transfer	13.2											
9.2.1	Information Transfer Policies and Procedures	13.2.1											
9.2.1.1	Direct Internet Access		1.3-1.3.7										
9.2.2	Agreements on Information Transfer	13.2.2		4									
9.2.2.1	Access Agreements for Information Transfer		164.308(a)(4)(i)										

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
9.2.3	Electronic Messaging	13.2.3		4									
9.2.3.1	Transmission Confidentiality					164.312(e)(1) & 164.312(e)(2)(i)		17.04(3)	622(2)(d)(C)(iii)				
9.2.3.2	Ad-Hoc Transfers												
9.2.3.3	Communications Technologies												
9.2.3.4	Intranets												ID.AM-4 & PR.AC-3
9.2.4	Confidentiality or Non-Disclosure Agreements (NDAs)	13.2.4											
9.2.4.1	Business Partner Contracts		2.6			164.308(b)(1), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-(B), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(1)-(2							
9.2.4.2	Third-Party Personnel Security												ID.AM-6, ID.GV-2, PR.AT-3 & PR.IP-11
9.2.4.3	Monitoring for Information Disclosure							17.04(3)					PR.PT-1 & DE.CM-3
10	Sytem Acquisition, Development and Maintenance Policy												
10.1	Security Requirements of Information Systems	14.1											
10.1.1	Information Security Requirements Analysis and Specification	14.1.1											
10.1.1.1	Secure Configurations		2.2-2.2.5		500.11								
10.1.2	Securing Application Services on Public Networks	14.1.2											
10.1.2.1	Software Firewall		1.4									2-5	
10.1.3	Protecting Application Services Transactions	14.1.3											
10.1.3.1	Transmission Integrity		4.1			164.312(e)(2)(i)							PR.DS-2 & PR.DS-5
10.2	Security in Development and Support Processes	14.2											
10.2.1	Secure Development	14.2.1											
10.2.1.1	Application Development		6.3-6.3.2		500.08								
10.2.2	System Change Control Procedures	14.2.2											
10.2.2.1	Change Control		6.4-6.4.6										
10.2.2.2	Secure Coding Principles		6.5-6.5.10		500.08								
10.2.3	Technical Review of Applications After Operating Platform Changes	14.2.3											
10.2.3.1	Test, Validate & Document Changes												
10.2.3.2	Security Functionality Verification												
10.2.4	Restrictions on Changes to Software Packages	14.2.4											
10.2.4.1	Library Privileges												
10.2.5	Secure System Engineering Principles	14.2.5											
10.2.5.1	Secure System Engineering Principles		2.2										PR.IP-2
10.2.5.2	Ports, Protocols & Services Documentation												
10.2.6	Secure Development Environment	14.2.6											
10.2.6.1	Development Environments												
10.2.7	Outsourced Development	14.2.7											
10.2.7.1	External Service Providers		12.8.2 & 12.8.4		500.11	17.03(2)(f)(1)			622(2)(d)(A)(v)				ID.AM-4, PR.AT-3 & DE.CM-6
10.2.7.2	Developer Configuration Management					17.03(2)(d)(B)(i)							PR.IP-1, PR.IP-2 & PR.IP-3
10.2.8	System Security Testing	14.2.8											
10.2.8.1	Security Assessments							17.03(2)(h)	622(2)(B)(i)-(iv)				ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3
10.2.8.2	Plan of Action & Milestones (POA&M)												
10.2.9	System Acceptance Testing	14.2.9											
10.2.9.1	Security Authorization												
10.3	Test Data	14.3											
10.3.1	Protection of Test Data	14.3.1											
10.3.1.1	Use of Live Data		6.4 & 6.4.3					17.03(2)(d)(B)(i)					
10.3.1.2	Test Data Integrity												
10.3.1.3	Information Output Handling & Retention		3.1 & 10.7						622(2)(C)(i) & (iv)				
11	Supplier Relationships Policy												
11.1	Information Security in Supplier Relationships	15.1								7.1.2			
11.1.1	nformation Security Policy for Supplier Relationships	15.1.1								7.1.2			
11.1.1.1	Service Provider Management		12.8										
11.1.1.2	System Development Life Cycle (SDLC)												PR.IP-2
11.1.1.3	Acquisition Process												PR.IP-2 & DE.CM-6
11.1.1.4	Commercial Off-The-Shelf (COTS) Security Solutions												
11.1.1.5	Functional Properties of Security Controls												
11.1.1.6	Design & Implementation of Security Controls												
11.1.1.7	Development Methods												
11.1.1.8	Developer Documentation												ID.RA-1
11.1.1.8.1	Developer Documentation | Ports, Protocols & Services In Use												
11.1.1.8.2	Developer Documentation | Functional Properties of Security Controls												
11.1.1.8.3	Developer Documentation | External System Interfaces												
11.1.1.8.4	Developer Documentation | High-Level Design												
11.1.1.8.5	Developer Documentation | Low-Level Design												
11.1.1.8.6	Developer Documentation | Source Code												
11.1.2	Addressing Security Within Supplier Agreements	15.1.2								7.1.2			
11.1.2.1	Service Provider Accountability		12.9										

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
11.1.2.2	Validate as Genuine & Not Altered												
11.1.2.3	Limitation From Harm												
11.1.3	Information and Communication Technology Supply Chain	15.1.3											
11.1.3.1	Supply Chain Protection												ID.BE-1 & PR.IP-2
11.1.3.2	Acquisition Strategies, Tools & Methods												
11.1.3.3	Criticality Analysis												ID.AM-5, ID.BE-3, ID.BE-4, ID.BE-5, ID.RA-4 & ID.RM-3
11.1.3.4	Trustworthiness												
11.2	Supplier Service Delivery Management	15.2								7.2.4			
11.2.1	Monitoring and Review of Supplier Services	15.2.1								7.2.4			
11.2.1.1	Supplier Reviews												
11.2.1.2	Supplier Weakness or Deficiency Remediation												
11.2.1.3	Development Process, Standards & Tools		6.3, 6.5, 6.5.1-6.5.10										PR.IP-2
11.2.2	Managing Changes to Supplier Services	15.2.2								7.2.4			
11.2.2.1	Developer Configuration Management							17.03(2)(d)(B)(i)					PR.IP-1, PR.IP-2 & PR.IP-3
11.2.2.2	Developer Security Testing		6.4 & 6.4.4					17.03(2)(d)(B)(i)					ID.RA-1 & PR.IP-2
11.2.2.3	Developer Code Analysis		6.3, 6.3.1 & 6.3.2										
11.2.2.4	Developer Threat Analysis & Flaw Remediation		6.6										
12	Information Security Incident Management Policy												
12.1	Management of Information Security Incidents and Improvements	16.1		12						1.2.7			
12.1.1	Responsibilities and Procedures	16.1.1		12									
12.1.1.1	Incident Response		12.10-12.10.6	12	500.16								
12.1.1.2	Incident Response Training			12									
12.1.2	Reporting Information Security Events	16.1.2		12									
12.1.2.1	Incident Reporting		12.8.3	12	500.16 500.17	164.308(a)(6)(ii)		17.03(2)(j)	604(1)-(5)				RS.CO-2
12.1.3	Reporting Information Security Weaknesses	16.1.3		12									
12.1.3.1	Reporting Weaknesses		12.5.2	12									DE.AE-3, DE.AE-5, RS.AN-1 & RS.AN-4
12.1.3.2	Incident Reporting Assistance			12									
12.1.4	Assessment of and Decision on Information Security Events	16.1.4		12						1.2.7			
12.1.4.1	Integrated Information Security Analysis Team		12.10.3	12									
12.1.5	Response to Information Security Incidents	16.1.5		12						1.2.7			
12.1.5.1	Incident Response Plan (IRP)		12.8.3, 12.10, 12.10.1-12.10.6	12	500.16	164.308(a)(6)(ii)			622(2)(d)(B)(iii)				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 & RC.IM-2
12.1.6	Learning from Information Security Incidents	16.1.6								1.2.7			
12.1.6.1	Incident Response Lessons Learned					164.308(a)(6)(i)							
12.1.7	Collection of Evidence	16.1.7											
12.1.7.1	Incident Handling		12.5.3		500.16								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
12.1.7.2	Information Spillage Response												
13	Business Continuity Management Policy												
13.1	Information Security Continuity	17.1											
13.1.1	Planning Information Security Continuity	17.1.1											
13.1.1.1	Contingency Plan					164.308(a)(7)(ii)(C) & 164.312(a)(2)(ii)							RS.CO-1
13.1.1.2	Contingency Training												
13.1.2	Implementing Information Security Continuity	17.1.2											
13.1.2.1	Contingency Planning Procedures					164.308(a)(7)(i)							ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-5, PR.DS-4, PR.IP-7, PR.IP-9, 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
13.1.3	Verify, Review and Evaluate Information Security Continuity	17.1.3											
13.1.3.1	Contingency Testing & Exercises					164.308(a)(7)(ii)(D)							
13.1.3.2	Contingency Plan Update					164.308(a)(7)(ii)(E)							PR.IP-4 & PR.IP-10
13.2	Redundancies	17.2											
13.2.1	Availability of Information Processing Facilities	17.2.1											
13.2.1.1	Alternate Storage Site					164.310(a)(2)(i)							PR.IP-4
13.2.1.2	Alternate Processing Site												
13.2.1.3	Telecommunications Services												ID.BE-4 & PR.PT-4
13.2.1.4	Priority of Service Provisions Storage Site												
14	Compliance Policy												

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	PCI DSS v3.2	FAR 52.204-21	NY DFS	HIPAA	GLBA	MA 201 CMR 17.00	OR 646A	GAPP	UK Data Protection	UK Cyber Essentials	NIST CSF
14.1	Compliance with Legal and Contractual Requirements	18.1								1.2.2 1.2.11			
14.1.1	Identification of Applicable Legislation and Contractual Requirements	18.1.1								1.2.11			
14.1.1.1	Regulatory & Non-Regulatory Compliance		12.1			164.308(a)(8)	6801(b)(3)						ID.BE-2, ID.BE-4, ID.GV-3 & ID.RM-3
14.1.2	Intellectual Property Rights	18.1.2											
14.1.2.1	Software Usage Restrictions												DE.CM-3
14.1.3	Protection of Records	18.1.3											
14.1.3.1	Minimizing Sensitive Data Storage		3.1										
14.1.3.2	Data Masking		3.3										
14.1.3.3	Storing Authentication Data		3.2-3.2.3										
14.1.3.4	Making Sensitive Data Unreadable In Storage		3.4-3.4.1										
14.1.4	Privacy and Protection of Personally Identifiable Information	18.1.4											
14.1.4.1	Minimization Of Personally Identifiable Information (PII)										Chapter29-Schedule1-Part1-Principle 3		
14.1.4.2	Data Retention & Disposal										Chapter29-Schedule1-Part1-Principle 5		
14.1.4.3	Data Collection												
14.1.4.4	Sensitive Data Storage		3.2 & 3.2.1-3.2.3										
14.1.5	Regulation of Cryptographic Controls	18.1.5											
14.1.5.1	Export-Controlled Information												
14.2	Information Security Reviews	18.2								1.2.5			
14.2.1	Independent Review of Information Security	18.2.1								1.2.5			
14.2.1.1	Independent Assessors												
14.2.2	Compliance with Security Policies and Standards	18.2.2								8.2.7 10.2.3			
14.2.2.1	Security Assessments							17.03(2)(h)	622(2)(B)(i)-(iv)				ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3
14.2.3	Technical Compliance Review	18.2.3								8.2.7 10.2.3			
14.2.3.1	Functional Properties Of Security Controls												