Policy Title	Standard #	Standard Title	Target Audience	Applicability	Relative Control Weighting (1-10)	SCF #	Secure Controls Framework (SCF) Control Description	AICPA SOC 2 (2016)	AICPA SOC 2 (2017)	CIS CSC v6.1	CIS CSC v7 (draft)	COBIT v5	COSO v2013	CSA CCM v3.0.1	ENISA v2.0	GAPP	ISO 27001 v2013	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-160	NIST 800-171 rev 1	NIST CSF	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US FFIEC	US FINRA	US GLBA	US HIPAA	US Privacy Shield	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US - TX BCS21	US-TX Cybersecurity Act	EMEA EU GDPR
Security & Privacy Governance	GOV-1	Publishing Security Policies	Management	Basic	10	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.					APO13.01 APO13.02	Principle 12	AIS-04 GRM-05 GRM-06	SO1	8.2.1	5.2	5.1.1	PM-1			ID.GV-1		12.1 12.1.1	§ 1232h	D1.G.SP.B.4	S-P (17 CFR §248.30)	6801(b)(1)	164.308(a)(1)(i) 164.316		17.03(1) 17.04 17.03(2)(b)(2)	500.03			Sec 10	Art 32.1 Art 32.2 Art 32.3 Art 32.4
Security & Privacy Governance	GOV-2	Assigned Security Responsibilities	Management	Basic	10	GOV-04	Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	CC1.1	CC1.1			APO01.06	Principle 2	GRM-05		8.2.7	5.3		PL-9 PM-2 PM-6			ID.AM-6		12.5-12.5.5		D1.R.St.B.1 D1.TC.Cu.B.1		Safeguards Rule	164.308(a)(2) 164.308(a)(3) 164.308(a)(4) 164.308(b)(1) 164.314		17.03(2)(a)	500.04	622(2)(d)(A)(i)		Sec 9	
Security & Privacy Governance	GOV-3	Measures of Performance	Management	Basic	6	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.					EDM02.03 APO01.04 EDM05.02 EDM05.03 MEA01.01 MEA01.03	Principle 5 Principle 9 Principle 13 Principle 14 Principle 15		SO11 S12 S13 S14 S15		9.1		PM-6	3.3.7 3.3.8		PR.IP-8				D2.IS.Is.B.1 D2.IS.Is.E.2			164.308(a)(6)(ii) 164.308(a)(8)		17.03(2)(j)		622(2)(d)(A)(vi) 622(2)(d)(B)(iii)		Sec 10 Sec 11	
Asset Management	AST-1	Asset Inventories	Management	Basic	10	AST-02	Mechanisms exist to inventory system components that: • Accurately reflects the current system; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed			1.4	1.6 2.1 2.5 12.9 16.12	BAI09.01 BAI09.05			SO15			8.1.1	CM-8 PM-5		3.4.1 3.4.2	ID.AM-1 ID.AM-2 ID.AM-4		1.1.2 2.2.4		D1.G.IT.B.1 D4.RM.Dd.B.2 D4.C.Co.B.3			164.308(a)(1)(ii)(A) 164.308(a)(4)(ii)(A) 164.308(a)(7)(ii)(E) 164.308(b) 164.310(d) 164.310(d)(2)(iii)								
Asset Management	AST-2	Network Diagrams & Data Flow Diagrams (DFDs)	Technical	Basic	10	AST-04	Mechanisms exist to maintain network architecture diagrams that: • Contain sufficient detail to assess the security of the network's architecture; • Reflect the current state of the network environment; and				12.9 16.12			IVS-13				PL-2 SA-5(1) SA-5(2) SA-5(3) SA-5(4)			ID.AM-3		1.1.2 1.1.3		D4.C.Co.B.4 D4.C.Co.Int.1			164.308(a)(1)(ii)(A) 164.308(a)(3)(ii)(A) 164.308(a)(8) 164.310(d)							Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5
Asset Management	AST-3	Removal of Assets	All Users	Basic	8	AST-11	Mechanisms exist to authorize, control and track systems entering and exiting organizational facilities.							DCS-04				11.2.5				PR.DS-3				D1.G.IT.E.3 D1.G.IT.E.2			164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)				622(2)(d)(C)(ii)			
Business Continuity & Disaster Recovery	BCD-1	Contingency Plan	Management	Basic	10	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls.	A1.3	A1.3			DSS04.01 DSS04.02 DSS04.03		BCR-01 BCR-07	SO19 SO20			17.1.2	CP-1 CP-2 IR-4(3) PM-8			RC.RP-1				D5.IR.Pl.B.6			164.308(a)(7) 164.308(a)(7)(i) 164.308(a)(7)(ii) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)							Art 32.1 Art 32.2
Business Continuity & Disaster Recovery	BCD-2	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	Management	Basic	9	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.					DSS04.05 DSS04.08			SO20 SO22				CP-4			RC.IM-1				D5.IR.Pl.Int.4			164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)							
Business Continuity & Disaster Recovery	BCD-3	Contingency Plan Update	Management	Basic	10	BCD-06	Mechanisms exist to keep contingency plans current with business needs and technology changes.					DSS04.08			SO19 SO20				CP-2			RC.IM-2				D5.IR.Pl.Int.4 D5.IR.Te.Int.5			164.308(a)(7)(ii)(D) 164.308(a)(8)							
Business Continuity & Disaster Recovery	BCD-4	Data Backups	Technical	Basic	10	BCD-11	Mechanisms exist to create recurring backups of data, software and system images to ensure the availability of the data.			10.1	10.1	DSS04.07						12.3.1	CP-9 SC-28(2)		3.8.9	PR.IP-4						164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(D) 164.310(a)(2)(i) 164.310(d)(2)(iv)								
Business Continuity & Disaster Recovery	BCD-5	Information System Recovery & Reconstitution	Technical	Basic	10	BCD-12	Mechanisms exist to ensure the recovery and reconstitution of systems to a known state after a disruption, compromise or failure.				10.5								CP-10			PR.IP-4				D5.IR.Pl.B.5 D5.IR.Te.E.3			164.308(a)(7)(ii)(B)							
Capacity & Performance Planning	CAP-1	Capacity & Performance Management	Management	Basic	8	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance for future capacity requirements.	A1.1	A1.1					IVS-04				12.1.3	SC-5 SC-5(3)			PR.DS-4				D5.IR.Pl.B.5 D5.IR.Pl.B.6 D5.IR.Pl.E.3 D3.PC.Im.E.4			164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7) 164.310(a)(2)(i) 164.310(d)(2)(iv) 164.312(a)(2)(ii)							Art 32.1 Art 32.2
Change Management	CHG-1	Configuration Change Control	All Users	Basic	10	CHG-02	Mechanisms exist to govern the technical configuration change control processes.							MOS-15	SO14			14.2.2	CM-3	3.4.10 3.4.13	3.4.3	PR.IP-3		6.4-6.4.6		D1.G.IT.B.4									
Compliance	CPL-1	Statutory, Regulatory & Contractual Compliance	All Users	Basic	10	CPL-01	Mechanisms exist to facilitate the implementation of relevant legislative statutory, regulatory and contractual controls.					MEA03.01 MEA03.02			SO25			18.1.1	PM-8	3.3 3.3.3 3.3.4 3.4 3.4.1 3.4.2		ID.GV-3 PR.IP-5		12.1		D1.G.Ov.E.2 D3.PC.Am.B.11		6801(b)(3)	164.306 164.308 164.308(a)(7)(i) 164.308(a)(7)(ii)(C) 164.308(a)(8) 164.310			500.19				Art 1.2 Art 2.1 Art 2.2 Art 3.1 Art 3.2 Art 3.3
Compliance	CPL-2	Security Controls Oversight	Management	Basic	10	CPL-02	Mechanisms exist to provide a security controls oversight function.					APO01.03 DSS01.04 DSS06.04 MEA02.01 MEA02.02		AAC-02 AAC-03	SO25	8.2.7	9.3		CA-7 CA-7(1) PM-14	3.3.8	3.12.1 3.12.2 3.12.3 3.12.4 NFO	DE.DP-5 PR.IP-7		12.11 12.11.1		D5.IR.Pl.Int.3 D1.RM.RMP.E.2 D1.G.Ov.A.2			164.306(e) 164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)				622(2)(B)(iii)		Sec 10 Sec 11	Art 5.2
Configuration Management	CFG-1	System Hardening Through Baseline Configurations	Technical	Basic	10	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.			3.1	5.1 5.2 5.3 5.5 6.2 8.3	BAI10.02		GRM-01 IVS-07				14.1.1	CM-2 CM-6 SA-8	3.4.7 3.4.8	3.4.1 3.4.2	PR.IP-1 PR.IP-3	A1 A2 A3 A4 A5 A6	1.1 1.1.1 2.2-2.2.4		D3.PC.Im.B.5 D1.G.IT.B.4			164.308(a)(8) 164.308(a)(7)(i) 164.308(a)(7)(ii)							
Configuration Management	CFG-2	Least Functionality	Technical	Basic	10	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.			9.1	9.1 9.5 15.7 15.8			IAC-03					CM-7		3.4.6	PR.PT-3	A6	1.1.5 1.2.1 2.2.2 2.2.4 2.2.5		D3.PC.Am.B.7 D3.PC.Am.B.4 D3.PC.Am.B.3 D4.RM.Om.Int.1			164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(2)(i)		17.03(2)(a) 17.03(2)(g)					
Monitoring	MON-1	Continuous Monitoring	Technical	Basic	10	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.			4.6	6.2 14.7	DSS01.03 DSS05.07		IVS-06	SO21			12.4.1	AU-1 SI-4		NFO	DE.CM-1 DE.DP-1 DE.DP-2 PR.PT-1	A2 A5 A10	10.1 10.6-10.6.3 10.8-10.8.1		D3.DC.An.B.2 D3.DC.An.B.3 D1.G.SP.B.3 D2.MA.Ma.B.1 D2.MA.Ma.B.2 D3.DC.Ev.B.4			164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(2) 164.308(a)(3)(ii)(A)				500.06			Art 32.1 Art 32.2
Monitoring	MON-2	Monitoring Reporting	Technical	Basic	7	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.			6.4									AU-7 AU-7(1) AU-12		3.3.1 3.3.2 3.3.6	DE.DP-4				D3.DC.Ev.B.2 D5.ER.Is.B.1 D5.ER.Is.E.1			164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)							
Monitoring	MON-3	Anomalous Behavior	Technical	Basic	10	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.			16.10	16.8								SI-4(11)			DE.AE-1		10.6-10.6.2		D3.DC.Ev.B.1 D4.C.Co.B.4			164.308(a)(1)(ii)(D) 164.312(b)							

Policy Title	Standard #	Standard Title	Target Audience	Applicability	Relative Control Weighting (1-10)	SCF #	Secure Controls Framework (SCF) Control Description	AICPA SOC 2 (2016)	AICPA SOC 2 (2017)	CIS CSC v6.1	CIS CSC v7 (draft)	COBIT v5	COSO v2013	CSA CCM v3.0.1	ENISA v2.0	GAPP	ISO 27001 v2013	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-160	NIST 800-171 rev 1	NIST CSF	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US FFIEC	US FINRA	US GLBA	US HIPAA	US Privacy Shield	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US - TX BC521	US-TX Cybersecurity Act	EMEA EU GDPR
Monitoring	MON-4	Insider Threats	Technical	Enhanced	8	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.															DE.CM-3				D3.DC.An.A.3			164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.308(a)(5)(ii)(C) 164.312(a)(2)(i) 164.312(b) 164.312(d)								
Monitoring	MON-5	Third-Party Threats	Technical	Enhanced	8	MON-16.2	Mechanisms exist to monitor third-party personnel activity for potential security incidents.															DE.CM-6				D4.RM.Om.Int.1			164.308(a)(1)(ii)(D)								
Monitoring	MON-6	Unauthorized Activities	Technical	Enhanced	8	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices, and software.															DE.CM-7				D3.DC.Ev.B.3			164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii)								
Cryptographic Protections	CRY-1	Transmission Confidentiality	Technical	Basic	10	CRY-03	Cryptographic mechanisms are utilized to protect the confidentiality of data being transmitted.		C1.3		11.4 13.2 14.2					8.2.5		13.2.3	SC-8 SC-9			PR.DS-2				D3.PC.Am.B.13 D3.PC.Am.E.5 D3.PC.Am.Int.7			164.308(b)(1) 164.308(b)(2) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii) 164.314(b)(2)(i)		17.04(3)	500.15	622(2)(d)(C)(iii)				Art 5.1
Cryptographic Protections	CRY-2	Transmission Integrity	Technical	Basic	10	CRY-04	Cryptographic mechanisms are utilized to protect the integrity of data being transmitted.				14.2							14.1.3	SC-8 SC-16(1) SC-28(1)		3.8.6 3.13.8 3.13.16	PR.DS-8		3.4 3.4.1 4.1 9.8.2					164.312(e)(2)(i) 164.312(e)(1) 164.312(e)(2)(i)		17.04(3)		622(2)(d)(C)(iii)				Art 5.1
Cryptographic Protections	CRY-3	Encrypting Data At Rest	All Users	Basic	10	CRY-05	Cryptographic mechanisms are utilized on systems to prevent unauthorized disclosure of information at rest.			14.5	13.2 13.10 14.5							10.1.1	SC-13 SC-28(2)			PR.DS-1		3.4 3.4.1		D1.G.IT.B.13 D3.PC.Am.B.14 D4.RM.Co.B.1 D3.PC.Am.A.1			164.308(a)(1)(ii)(D) 164.308(b)(1) 164.310(d) 164.312(a)(1) 164.312(a)(2)(iii) 164.312(a)(2)(iv)		17.04(5)	500.15	622(2)(d)(C)(iii)				Art 5.1
Data Classification & Handling	DCH-1	Data & Asset Classification	All Users	Basic	10	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.			13.1	13.1	BAI08.03		DSI-01 DCS-01				8.2.1				ID.AM-5		9.6.1		D1.G.IT.B.2			164.308(a)(7)(ii)(E)							
Data Classification & Handling	DCH-2	Physical Media Disposal	All Users	Basic	10	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	C1.8	C1.8					DSI-07				8.3.2	MP-6	3.4.14		PR.IP-6				D1.G.IT.B.19			164.310(d)(2)(i) 164.310(d)(2)(ii)				Sec. 521.052(b)		
Data Classification & Handling	DCH-3	Removable Media Security	All Users	Basic	10	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.				13.4							8.3.1				PR.PT-2				D1.G.SP.B.4 D3.PC.De.B.1 D3.PC.Im.E.3			164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2) 164.312(a)(1) 164.312(a)(2)(iv)								
Endpoint Security	END-1	Malicious Code Protection (Anti-Malware)	All Users	Basic	10	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	CC5.8	CC5.8	8.1	8.1 8.6 8.8	DSS05.01		TVM-01	SO12			12.2.1	SI-3		3.14.1 3.14.2 3.14.3 3.14.4 3.14.5	DE.CM-4		5.1-5.1.2 5.2 5.3		D3.DC.Th.B.2			164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)		17.04(7)						
Endpoint Security	END-2	File Integrity Monitoring (FIM)	Technical	Enhanced	8	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM) technology to detect and report unauthorized changes to system files and configurations.			3.5					SO12				SI-7			PR.DS-6		11.5-11.5.1		D3.PC.Se.Int.3 D3.PC.De.Int.2			164.308(a)(1)(ii)(D) 164.312(b) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)								
Endpoint Security	END-3	Mobile Code	Technical	Basic	4	END-10	Mechanisms exist to address mobile code / operating system-independent applications.							TVM-03					SC-18 SC-18(1) SC-18(2) SC-18(3) SC-18(4) SC-27		3.13.13	DE.CM-5				D3.PC.De.E.5			164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)								
Human Resources Security	HRS-1	Human Resources Security Management	All Users	Basic	10	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.					APO04.01			SO7 SO8				PS-1	3.2.4	NFO	PR.IP-11				D1.R.St.E.4			164.308(a)(1)(ii)(C) 164.308(a)(3)							Art 32.1 Art 32.2 Art 32.4
Identification & Authentication	IAC-1	User Provisioning & De-Provisioning	All Users	Basic	10	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	CC5.2	CC5.2		16.3			IAC-09 IAC-11	SO7			9.2.1-9.2.2	IA-5(3)			PR.AC-6	AS												
Identification & Authentication	IAC-2	Account Management	All Users	Basic	10	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, application, guest and temporary accounts.				16.1 16.4 16.13			IAC-10		8.2.2			AC-2		3.1.1 3.1.2	PR.AC-1		8.1.3-8.1.5 8.2.2 8.5-8.5.1 8.6 8.7		D3.PC.Im.B.7 D3.PC.Am.B.6			164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i)		17.04(1)(a)						
Identification & Authentication	IAC-3	Least Privilege	All Users	Basic	10	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	CC5.6	CC5.6		14.4				SO11			9.1.2	AC-6		3.1.5	PR.AC-4	AS			D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5			164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i)				622(2)(d)(C)(iii)				
Incident Response	IRO-1	Management of Security Incidents	Management	Basic	10	IRO-01	Mechanisms exist to facilitate the implementation of incident response controls.								SO16 SO18	1.2.7		16.1.1	IR-1		NFO	PR.IP-9				DS.IR.PI.B.1			164.308(a)(6) 164.308(a)(6)(i) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)			500.16			Sec 8	Art 32.1 Art 32.2
Incident Response	IRO-2	Incident Handling	All Users	Basic	10	IRO-02	Incident handling mechanisms exist to cover preparation, detection and analysis, containment, eradication and recovery.					DSS02.03 DSS02.04 DSS02.05 DSS02.06. DSS03.01 DSS03.02				1.2.7		16.1.4	IR-4		3.6.1 3.6.2	DE.AE-2 DE.AE-4 DE.AE-5 RS.AN-1 RS.AN-4 RS.MI-1		12.5.3 12.10		DS.IR.PI.Int.4 DS.IR.Te.E.1 DS.ER.Es.E.1 D1.RM.RMP.A.4 DS.DR.De.B.1 D3.DC.An.E.4			164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(6)(i) 164.308(a)(6)(ii)						Sec 8	
Incident Response	IRO-3	Indicators of Compromise (IOC)	Technical	Basic	8	IRO-03	Mechanisms exist to define specific indicators of Compromise (IOC) that identify the potential impact of likely cybersecurity events.															RS.AN-2				D1.RM.RMP.A.4 DS.IR.Te.E.1 DS.ER.Es.E.1			164.308(a)(6)(ii) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)K								
Incident Response	IRO-4	Incident Response Plan (IRP)	Technical	Basic	8	IRO-04.2	Mechanisms exist to regularly update incident response strategies to keep current with business needs, technology changes and regulatory requirements.												IR-1		NFO	RS.IM-2				DS.IR.PI.Int.4 DS.IR.Te.Int.5			164.308(a)(7)(ii)(D) 164.308(a)(8)								

Policy Title	Standard #	Standard Title	Target Audience	Applicability	Relative Control Weighting (1-10)	SCF #	Secure Controls Framework (SCF) Control Description	AICPA SOC 2 (2016)	AICPA SOC 2 (2017)	CIS CSC v6.1	CIS CSC v7 (draft)	COBIT v5	COSO v2013	CSA CCM v3.0.1	ENISA v2.0	GAPP	ISO 27001 v2013	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-160	NIST 800-171 rev 1	NIST CSF	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US FFIEC	US FINRA	US GLBA	US HIPAA	US Privacy Shield	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR §46A	US - TX BCS21	US-TX Cybersecurity Act	EMEA EU GDPR
Incident Response	IRO-5	Coordination with Related Plans	Technical	Enhanced	7	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.									1.2.7			IR-3(2)			PR.IP-10				DS.IR.Te.B.1 DS.IR.Te.B.3			164.308(a)(7)(ii)(D)								
Incident Response	IRO-6	Integrated Security Incident Response Team (ISIRT)	Technical	Basic	10	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and privacy incident response operations.					DSS02.05				SO16			16.1.4	IR-10			RC.CO-1 RC.CO-2 RC.CO-3 RS.CO-1 RS.CO-4		12.10.3		DS.ER.Es.Int.3 DS.IR.Pl.Int.1 DS.IR.Pl.B.3 DS.ER.Is.B.1 DS.IR.Pl.Int.1			164.308(a)(2) 164.308(a)(6) 164.308(a)(ii)(i) 164.308(a)(6)(ii) 164.308(a)(7) 164.308(a)(7)(ii)(A)					Sec. 521.053	Sec 8 Sec 9	Art 34.1 Art 34.2 Art 34.3 Art 34.4
Incident Response	IRO-7	Chain of Custody & Forensics	Technical	Basic	10	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody.											16.1.7				RS.AN-3				D3.CC.Re.Int.3 D3.CC.Re.Int.4			164.308(a)(6)								
Incident Response	IRO-8	Incident Monitoring & Tracking	Technical	Basic	8	IRO-09	Mechanisms exist to document, monitor and report cybersecurity and privacy incidents.							SEF-05	SO17	1.2.7			IR-5		3.6.1 3.6.2	DE.AE-3		12.5.2 12.10.5		D3.DC.Ev.E.1			164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.308(a)(8) 164.310(d)(2)(iii)								
Incident Response	IRO-9	Incident Reporting	All Users	Basic	9	IRO-10	Mechanisms exist to report incidents: • Internally to organizational incident response personnel within organization-defined time-periods; and • Externally to regulatory authorities and affected parties, as necessary.	CC2.5	CC2.5	19.4 19.6		DSS02.07 DSS03.03			SO18	1.2.7		16.1.2 16.1.3	IR-6		3.6.1 3.6.2	RS.CO-2 RS.CO-3 RS.CO-5		12.5.2 12.8.3		DS.IR.Pl.B.2 DS.DR.Re.B.4 DS.DR.Re.E.6 DS.ER.Es.B.4 DS.ER.Es.B.2 DS.IS.Is.B.3			164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(ii)			17.03(2)(j)	500.17	604(1)-(5)	Sec. 521.053	Sec 8	Art 33.1 Art 33.2 Art 33.3 Art 33.4 Art 33.5 Art 34.1
Incident Response	IRO-10	Root Cause Analysis (RCA) & Lessons Learned	Technical	Basic	10	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents.					DSS03.04			SO18			16.1.6	IR-1		NFO	RS.IM-1		12.10.6		D5.IR.Pl.Int.4			164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)								
Maintenance	MNT-1	Controlled Maintenance	All Users	Basic	10	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.												MA-2	3.4.13	3.7.1 3.7.2 3.7.3	PR.MA-1	A9			D3.CC.Re.Int.5 D3.CC.Re.Int.6			164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)								
Maintenance	MNT-2	Non-Local Maintenance	Technical	Basic	10	MNT-05	Mechanisms exist to authorize, monitor and control non-local maintenance and diagnostic activities.												MA-4	3.4.13	3.7.5	PR.MA-2				D3.PC.Im.B.7			164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2)(i) 164.310(d)(2)(iii) 164.312(a) 164.312(a)(2)(ii)								
Network Security	NET-1	Network Security Management	All Users	Basic	10	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of network security controls.				11.1 11.2	DSS05.02						13.1.1 13.1.2	SC-1		NFO	PR.PT-4				D3.PC.Im.B.1 D3.PC.Am.B.11 D3.PC.Im.Int.1			164.308(a)(1)(ii)(D) 164.312(a)(1) 164.312(b) 164.312€								Art 32.1 Art 32.2
Network Security	NET-2	Layered Network Defenses	Technical	Basic	9	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.			9.5												PR.AC-5		1.3.7		D3.DC.Im.B.1 D3.DC.Im.Int.1			164.308(a)(4)(ii)(B) 164.310(a)(1) 164.310(b) 164.312(a)(1) 164.312(b) 164.312(c)								
Network Security	NET-3	Remote Access	All Users	Basic	10	NET-14	Mechanisms exist to define, control and review remote access methods.			12.7	12.6 12.7							6.2.2	AC-17 AC-17(6)		3.1.1 3.1.2	PR.AC-3		12.3.8 12.3.9		D3.PC.Am.B.15 D3.PC.De.E.7 D3.PC.Im.Int.2			164.308(a)(4)(i) 164.308(b)(1) 164.308(b)(3) 164.310(b) 164.312(e)(1) 164.312(e)(2)(ii)								
Physical & Environmental Security	PES-1	Physical Access Control	All Users	Basic	10	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).					DSS05.05 DSS05.06		DCS-02	SO9			9.1.1	PE-3 PE-3(2) PE-3(3)		3.10.3 3.10.4 3.10.5	PR.AC-2		9.1-9.1.2 9.2 9.4.2 9.4.3		D3.PC.Am.B.11 D3.PC.Am.B.17			164.308(a)(1)(ii)(B) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.310(a)(1) 164.310(a)(2)(i) 164.310(a)(2)(ii)			17.03(2)(g)		622(2)(d)(C)(ii)			
Physical & Environmental Security	PES-2	Monitoring Physical Access	Management	Basic	10	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.					DSS05.07			SO9				PE-6		3.10.1 3.10.2	DE.CM-2		9.1 -9.1.1		D3.PC.Am.E.4 D3.Dc.Ev.B.5			164.310(a)(2)(iv) 164.310(a)(2)(iii) 164.310(c)			622(2)(d)(C)(ii)					
Physical & Environmental Security	PES-3	Information Leakage Due To Electromagnetic Signals Emanations			5	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.															PR.DS-5				D3.PC.Am.B.15 D3.PC.Am.Int.1 D3.PC.De.Int.1 D3.DC.Ev.Int.1			164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a)								
Project & Resource Management	PRM-1	Allocation of Resources	Management	Basic	10	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and privacy requirements within business process planning for projects / initiatives.					BAI05.04 APO07.01						7.1	SA-2	3.2 3.2.1 3.2.2 3.2.3 3.2.4 3.2.5	NFO	ID.BE-3				D1.G.SP.E.2 D1.G.Ov.Int.5 D1.G.SP.Int.3			164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.310(a)(2)(i) 164.316						Sec 12	
Project & Resource Management	PRM-2	Security Requirements Definition	Management	Basic	10	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the System Development Lifecycle (SDLC).	CC2.2	CC2.2			DSS06.01	Principle 10 Principle 11					14.1	SA-14	3.4 3.4.3 3.4.4 3.4.5 3.4.6		ID.BE-4 ID.BE-5				D4.C.Co.B.1 D1.G.IT.B.2 D5.IR.Pl.B.5 D5.IR.Pl.E.3			164.308(a)(1)(ii)(B) 164.308(a)(6)(ii) 164.308(a)(7) 164.308(a)(7)(i) 164.308.a(7)(ii)(E) 164.308(a)(8)						Sec 12	
Project & Resource Management	PRM-3	System Development Life Cycle (SDLC) Management	Management	Basic	10	PRM-07	Mechanisms exist to ensure changes to systems within the System Development lifecycle (SDLC) are controlled through formal change control procedures.	CC7.1	CC7.1			APO04.06 BAI01.02 BAI01.03 BAI01.04 BAI01.05 BAI01.06	Principle 2			7.1 7.2 7.3 7.4 7.5	14.2.2	SA-3	3.2.1	NFO	PR.IP-2				D3.PC.Se.B.1 D3.PC.Se.E.1			164.308(a)(1)(i)						Sec 12	
Risk Management	RSK-1	Risk Management Program	All Users	Basic	10	RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.						Principle 6		SO2				11.1.4	PM-9 RA-1	3.3.4	NFO	ID.GV-4 ID.RM-1 ID.RM-2 ID.RM-3		12.2		D1.G.Ov.B.1 D1.G.Ov.B.3 D1.G.Ov.E.1 D1.G.SP.E.1 D1.G.Ov.Int.1 D1.G.Ov.Int.3		6801(b)(2)	164.308(a)(1) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(B) 164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(C)			17.03(2)(b)	500.09	622(2)(d)(A)(ii)		Sec 7	Art 32.1 Art 32.2
Risk Management	RSK-2	Risk Identification	All Users	Basic	10	RSK-03	Mechanisms exist to identify and document risks, both internal and external.				3.5		Principle 7									ID.RA-3				D3.DC.An.B.1 D2.MA.Ma.E.1 D2.MA.Ma.E.4 D2.MA.Ma.Int.2			164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.308(a)(5)(ii)(A) 164.310(a)(1)						Sec 7	
Risk Management	RSK-3	Risk Assessment	All Users	Basic	10	RSK-04	Mechanisms exist to conduct an annual assessment of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.				3.5	DSS06.04	Principle 7 Principle 8	BCR-05 GRM-02 GRM-10	SO2	1.2.4	8.2	11.1.4	RA-3		3.11.1	ID.RA-5		12.2		D1.RM.RA.B.1 D1.RM.RA.E.2 D1.RM.RA.E.1		Safeguards Rule	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.316(a)			17.03(2)(b)		622(b)(A)(ii)		Sec 7 Sec 11	Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9

Policy Title	Standard #	Standard Title	Target Audience	Applicability	Relative Control Weighting (1-10)	SCF #	Secure Controls Framework (SCF) Control Description	AICPA SOC 2 (2016)	AICPA SOC 2 (2017)	CIS CSC v6.1	CIS CSC v7 (draft)	COBIT v5	COSO v2013	CSA CCM v3.0.1	ENISA v2.0	GAPP	ISO 27001 v2013	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-160	NIST 800-171 rev 1	NIST CSF	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US FFIEC	US FINRA	US GLBA	US HIPAA	US Privacy Shield	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US - TX BCS21	US-TX Cybersecurity Act	EMEA EU GDPR
Risk Management	RSK-4	Risk Remediation	All Users	Basic	10	RSK-06	Mechanisms exist to remediate risks to an acceptable level.						Principle 9	GRM-11			8.3 10.1					ID.RA-6				DS.IR.PI.B.1 DS.DR.Re.E.1 DS.IR.PI.E.1			164.308(a)(1)(ii)(B) 164.314(a)(2)(i)(C) 164.314(b)(2)(iv)								
Risk Management	RSK-5	Business Impact Analysis (BIAs)	All Users	Basic	10	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIAs).					BAI01.10 BAI02.03	Principle 7 Principle 8	BCR-08 BCR-09			8.2					ID.RA-4				DS.RE.Re.B.1 DS.ER.Er.Ev.1			164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6) 164.308(a)(7)(ii)(E) 164.308(a)(8)								Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9
Secure Engineering & Architecture	SEA-1	Secure Engineering Principles	All Users	Basic	10	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security and privacy practices in the specification, design, development, implementation and modification of systems and services.	CC3.2	CC3.2			DSS06.06	Principle 10 Principle 11		SO12	4.2.3 6.2.2 7.2.2 7.2.3	14.2.5	AR-7 SA-8 SA-13 SC-7(18) SI-1	2.1 2.2 2.3 2.4	3.13.1 3.13.2 NFO	PR.IP-1	A5 A6	2.2						Principle 4				Sec. 521.052		Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2
Secure Engineering & Architecture	SEA-2	Fail Secure	Technical	Enhanced	8	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.												CP-12 SC-24			PR.PT-5	A5 A6												
Security Awareness & Training	SAT-1	Security & Privacy-Minded Workforce	All Users	Basic	10	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.					BAI08.04 BAI08.05		HRS-09	SO6			7.2.2	AT-1 PM-13		NFO	PR.AT-1 PR.AT-3 PR.AT-4				D1.TC.Tr.B.2 D1.TC.Tr.B.4 D1.TC.Tr.Int.2 D1.TC.Tr.E.2			164.308(a)(2) 164.308(a)(3)(i) 164.308(a)(5) 164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B)			500.14			Sec 6	Art 32.1 Art 32.2 Art 32.4
Security Awareness & Training	SAT-2	Security & Privacy Training	All Users	Basic	10	SAT-03	Mechanisms exist to provide role-based security-related training: • Before authorizing access to the system or performing assigned duties; • When required by system changes; and • Annually thereafter.			17.2					SO6				AT-3		3.2.1 3.2.2	PR.AT-2 PR.AT-5		12.6.1		D1.TC.Tr.E.3 D1.R.St.E.3			164.308(a)(2) 164.308(a)(3)(i) 164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C)		17.04(B)		622(2)(d)(A)(iv			
Security Awareness & Training	SAT-3	Privileged Users	Technical	Basic	10	SAT-03.5	Mechanisms exist to provides specific training for privileged users to ensure privileged users understand their unique roles and responsibilities															PR.AT-2 PR.AT-5				D1.TC.Tr.E.3 D1.R.St.E.3										
Technology Development & Acquisition	TDA-1	Separation of Development, Testing and Operational Environments	Technical	Basic	10	TDA-08	Mechanisms exist to manage separate development, testing, and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.			18.6				IVS-08				12.1.4	CM-4(1)			PR.DS-7		6.4.1		D3.PC.Am.B.10			164.308(a)(4)							
Third-Party Management	TPM-1	Third-Party Management	All Users	Basic	10	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	C1.5	C1.5			DSS01.02		IAC-07 STA-05 STA-09	SO4			15.1.1	SA-4		NFO	ID.SC-1	A3 A4	12.8								500.11			Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6
Third-Party Management	TPM-2	Third-Party Criticality Assesments	Management	Basic	10	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process.												SA-14			ID.BE-1 ID.SC-2				D1.G.SP.A.3			164.308(a)(1)(ii)(A) 164.308(a)(4)(ii) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(2)(i)								
Third-Party Management	TPM-3	Supply Chain Protection	All Users	Basic	10	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.							STA-01 STA-06	SO10			15.1.3	SA-12			ID.SC-4	A3 A4												Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6
Third-Party Management	TPM-4	Third-Party Contract Requirements	All Users	Basic	10	TPM-05	Mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization's needs to protect systems and data.	C1.4	C1.4									13.2.4 15.1.2	SA-9(3)			ID.SC-3		2.6 12.9					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)(i)(C)								Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6
Third-Party Management	TPM-5	Third-Party Personnel Security	All Users	Basic	10	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.															ID.GV-2				D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5			164.308(a)(1)(i) 164.308(a)(2) 164.308(a)(3) 164.308(a)(4) 164.308(b) 164.314								
Third-Party Management	TPM-6	Third-Party Incident Response & Recovery Capabilities	Technical	Enhanced	8	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.															ID.SC-5												
Threat Management	THR-1	Threat Awareness Program	Management	Basic	10	THR-01	Mechanisms exist to implement a threat awareness program that includes a cross-organization information-sharing capability.	CC3.1	CC3.1			BAI08.01							PM-16			ID.BE-2		12.6		D1.G.SP.Inn.1			164.308(a)(1)(ii)(A) 164.308(a)(4)(ii) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(2)(i)			500.10				Art 32.1 Art 32.2
Threat Management	THR-2	Threat Intelligence Feeds	Technical	Enhanced	10	THR-03	Mechanisms exist to maintain situational awareness of evolving threats.			4.4									SI-5 SI-5(1)		3.14.1 3.14.2 3.14.3	ID.RA-2		6.2 12.4		D2.TI.Ti.B.1			164.308(A)(5)(ii) (ii)(A)			622(2)(d)(B)(iii)			
Vulnerability & Patch Management	VPM-1	Vulnerability & Patch Management Program (VPMP)	All Users	Basic	10	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	CC6.1	CC6.1		11.5			TVM-02				12.6.1	SI-2 SI-3(2)			ID.RA-1 PR.IP-12	A6 A9			D2.TI.Ti.B.2 D3.DC.Th.B.1 D1.RM.RA.E.2 D3.DC.Th.E.5 D3.DC.Th.A.1 D3.CC.Re.Ev.2			164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(1)							Art 32.1 Art 32.2
Vulnerability & Patch Management	VPM-2	Continuous Vulnerability Remediation Activities	All Users	Basic	10	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.			9.4							10.2		SC-18(1)			RS.MI-3	A6 A9	6.6		D1.RM.RA.E.1			164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6)(ii)							
Vulnerability & Patch Management	VPM-3	Vulnerability Scanning	All Users	Basic	10	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by recurring vulnerability scanning of systems and web applications.			4.1	3.1 3.2 9.3 9.5 11.3			IVS-05					RA-5		3.11.2 3.11.3	DE.CM-8	A6 A9	11.2		D3.DC.Th.E.5			164.308(a)(1)(i) 164.308(a)(8)			500.05	622(2)(B)(iii) 622(2)(d)(A)(iii)			
Vulnerability & Patch Management	VPM-4	Red Team Exercises	Technical	Enhanced	3	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.			20.3 20.5 20.7									CA-8(2)			DE.DP-3				D3.DC.Ev.Int.2			164.306(e)							