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	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 v1.1	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 RCS21	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	§ 9 (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 MEA02.04	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		7.4.1	ID.AM-1 ID.AM-2 ID.AM-4		1.1.2 2.2.4		D1.G.IT.B.1 D4.RM.Od.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)					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				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)(iii)			
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-2 CP-2(1) CP-2(3)			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.								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)	164.308 164.308(a)(7)(i) 164.308(a)(7)(ii)(C) 164.308(a)(8) 164.310			500.19				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	3.1 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)(5) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1)		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)(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)(ii)							

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	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 v1.1	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
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)							
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			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	6.22(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	SC-8 SC-8(1)		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)		6.22(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								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	6.22(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								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)(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-03	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	A5													
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)(C) 164.308(a)(4)(ii) 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	A5			D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5			164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i)					6.22(2)(d)(C)(iii)			
Identification & Authentication	IAC-4	Identification & Authentication for Devices	Technical	Basic	8	IAC-04	Mechanisms exist to uniquely identify and authenticate devices before establishing a connection.		CC6.1		16.6								IA-3 IA-3(1) IA-3(4)		3.5.1	PR.AC-7													
Identification & Authentication	IAC-5	Multi-Factor Authentication (MFA)	Technical	Enhanced	8	IAC-06	Mechanisms exist to require Multi-Factor Authentication (MFA) for remote network access.			5.6 5.7 11.4 12.6 16.11 16.12	1.8 4.5 11.5 12.11 16.3							11.1.2	IA-2(11)			PR.AC-7	A2	8.3-8.3.2								500.12				