Policy #	ISO 27001-27002 Policy Title	ISO 27001-27002 Standard #	ISO 27001-27002 Standard Title	ISO 27001-27002 CSOP Procedure #	ISO 27001 v2013	ISO 27002 v2013	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	NIST CSF v1.1	NIST 800-53 rev5	PCIDSS v3.2	US FACTA	US FDA 21 CFR Part 11	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA EU GDPR	SCF #	Secure Controls Framework (SCF) Control Description
1	Security & Privacy Governance	GOV-01	Security & Privacy Governance Program	*P-GOV-01*	5.1 6.1.1	5.1.1	CC1.2			PM-1	12.1 12.1.1			§ 1232h	6801(b)(1)	164.306 164.306(a) 164.306(b) 164.306(c) 164.306(d) 164.306(e)	17.03(1) 17.04 17.03(2)(b)(2)	500.02		Sec 10	Art 32.1 Art 32.2 Art 32.3 Art 32.4	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.
		GOV-02	Steering Committee	*P-GOV-02*	6.2 7.4 9.3 10.2																	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.
		GOV-03	Publishing Security & Privacy Documentation	*P-GOV-03*	5.2 7.5.1 7.5.2 7.5.3	5.1.1	CC5.3		ID.GV-1	PM-1	12.1 12.1.1		§ 11.10 § 11.10(j)	§ 1232h	6801(b)(1)	164.306 164.308 164.308(a)(1)(i) 164.312 164.316 164.316(a)	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	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.
		GOV-04	Periodic Review & Update of Security & Privacy Program	*P-GOV-04*	6.1.1 7.4	5.1.2	CC5.3			PM-1				§ 1232h		164.306(b) 164.316(b) 164.316(b)(1) 164.316(b)(1)(i) 164.316(b)(1)(ii) 164.316(b)(2)(iii)				Sec 10	Art 32.1 Art 32.2 Art 32.3 Art 32.4	GOV-03	Mechanisms exist to review the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		GOV-05	Assigned Security & Privacy Responsibilities	*P-GOV-05*	5.3		CC1.1 CC1.3		ID.AM-6	PL-9 PM-2 PM-6 PM-29	12.5 12.5.1 12.5.2 12.5.3 12.5.4 12.5.5				Safeguards Rule	164.308(a)(2)	17.03(2)(a)	500.04	622(2)(d)(A)(i)	Sec 9		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.
		GOV-06	Measures of Performance	*P-GOV-06*	9.1		CC1.2 CC1.5 CC2.2		PR.IP-8	PM-6							17.03(2)(j)		622(2)(d)(A)(vi) 622(2)(d)(B)(iii)	Sec 10 Sec 11		GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.
		GOV-07	Contacts With Authorities	*P-GOV-07*		6.1.3	CC2.3	19.5		IR-6										Sec 5 Sec 11	Art 31 Art 36.1 Art 36.2 Art 36.3 Art 37.7 Art 40.1	GOV-06	Mechanisms exist to identify and document appropriate contacts within relevant law enforcement and regulatory bodies.
		GOV-08	Contacts With Groups & Associations	*P-GOV-08*		6.1.4		19.5		PM-15	5.1.2 6.1									Sec 5 Sec 11	Art 40.2 Art 41.1 Art 42.2 Art 42.3 Art 43.2	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: • Facilitate ongoing cybersecurity and privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity
2	Asset Management	AST-01	Asset Governance	*P-AST-01*		11.2.6		1.4 1.5 2.6		PM-5	12.3.3 12.3.4 12.3.7										Art 32.1 Art 32.2	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.
		AST-02	Asset Inventories	*P-AST-02*		8.1.1		1.4 1.5 1.6 2.1 2.5 16.1	ID.AM-1 ID.AM-2 ID.AM-4	CM-8 PM-5	1.1.2 22.4					164.310(d)(2)(iii)						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 necessary to achieve effective property accountability;
		AST-03	Software Licensing Restrictions	*P-AST-03*		18.1.2		2.1 2.10		SC-18(2)												AST-02.7	Mechanisms exist to ensure compliance with software licensing restrictions.
		AST-04	Assigning Ownership of Assets	*P-AST-04*		8.1.2				SA-4(12)	2.5											AST-03	Mechanisms exist to assign asset ownership responsibilities to a department, team or individual that establishes a common understanding of requirements to protect assets.
		AST-05	Security of Assets & Media	*P-AST-05*		11.2.6					9.6 9.6.1 9.6.2 9.6.3											AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive media.
		AST-06	Unattended End-User Equipment	*P-AST-06*		11.2.6 11.2.8																AST-06	Mechanisms exist to implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access.

Policy #	ISO 27001-27002 Policy Title	ISO 27001-27002 Standard #	ISO 27001-27002 Standard Title	ISO 27001-27002 CSOP Procedure #	ISO 27001 v2013	ISO 27002 v2013	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	NIST CSF v1.1	NIST 800-53 rev5	PCIDSS v3.2	US FACTA	US FDA 21 CFR Part 11	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA EU GDPR	SCF #	Secure Controls Framework (SCF) Control Description
2	Asset Management	AST-07	Kiosks & Point of Sale (PoS) Devices	*P-AST-07*		11.2.8					9.9 9.9.1 9.9.2 9.9.3											AST-07	Mechanisms exist to protect devices that capture sensitive data via direct physical interaction from tampering and substitution.
		AST-08	Tamper Detection	*P-AST-08*		11.2.6																AST-08	Mechanisms exist to inspect mobile devices for evidence of tampering upon return from geographic regions of concern or other known hostile environments that could lead to device compromise.
		AST-09	Secure Disposal, Destruction or Re-Use of Equipment	*P-AST-09*		11.2.7	CC6.5			SR-12	9.8 9.8.1 9.8.2					164.310(d)(2)(i) 164.310(d)(2)(ii)						AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.
		AST-10	Return of Assets	*P-AST-10*		8.1.4																AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.
		AST-11	Removal of Assets	*P-AST-11*		11.2.5			PR.DS-3							164.310(d)(1) 164.310(d)(2)			622(2)(d)(C)(ii)			AST-11	Mechanisms exist to authorize, control and track systems entering and exiting organizational facilities.
		AST-12	Tamper Protection	*P-AST-12*		11.2.6				SR-9 SR-9(1)												AST-15	Mechanisms exist to validate the integrity of configuration settings of critical systems, system components or services throughout all phases of the Secure Development Life Cycle (SDLC).
3	Business Continuity & Disaster Recovery	BCD-01	Business Continuity Management System (BCMS)	*P-BCD-01*		17.1.1 17.1.2	CC7.5 CC9.1		ID.BE-5 PR.IP-9 RC.RP-1	CP-1 CP-2 IR-4(3) PM-8 CP-10						164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(b)					Art 32.1 Art 32.2	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.
		BCD-02	Contingency Plan Testing & Exercises	*P-BCD-02*		17.1.3	CC7.5 A1.3			CP-4						164.308(a)(7)(ii)(D)						BCD-04	Mechanisms exist to conduct tests and/or exercises to determine the contingency plan's effectiveness and the organization's readiness to execute the plan.
		BCD-03	Alternate Storage Site	*P-BCD-03*		17.2.1	A1.2			CP-6 PE-23						164.310(a)(2)(i)						BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.
		BCD-04	Alternate Processing Site	*P-BCD-04*		17.2.1	A1.2			CP-7 PE-23						164.310(a)(2)(i)						BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.
		BCD-05	Data Backups	*P-BCD-05*		12.3.1	CC7.5 A1.2	10.1 10.2 10.4	PR.IP-4	CP-9 SC-28(2)						164.308(a)(7)(ii)(A) 164.310(d)(2)(iv)						BCD-11	Mechanisms exist to create recurring backups of data, software and system images to ensure the availability of the data.
		BCD-06	Testing for Reliability & Integrity	*P-BCD-06*		12.3.1	CC7.5 A1.2	10.3	PR.IP-4	CP-9(1)												BCD-11.1	Mechanisms exist to routinely test backups that verifies the reliability of the backup process, as well as the integrity and availability of the data.
		BCD-07	Separate Storage for Critical Information	*P-BCD-07*		12.3.1	A1.2	10.4 10.5		CP-9(3)												BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.
		BCD-08	Cryptographic Protection	*P-BCD-08*		12.3.1	A1.2	10.4		CP-9(8)												BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and modification of backup information.