CSA STAR 2 CONSENSUS ASSESSMENTS INITIATIVE

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers: Yes	No	Not Applicable	Notes	CCM v3.0.1 Compliance Mapping: AICPA TSC 2009	AICPA Trust Service Criteria (SOC 2SM Report)	AICPA TSC 2014	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	Canada PIPEDA	CCM V1.X	CIS-AWS-Foundations v1.1	COBIT 4.1	COBIT 5.0	COPPA	CSA Enterprise Architecture (formerly the Trusted Cloud Initiative): Domain > Container > Capability	Public	Private	CSA Guidance V3.0	ENISA IAF	EU 95/EC - European Union Data Protection Directive	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	FERPA	GAPP (Aug 2009)	HIPAA/HITECH (Omnibus Rule)	HITRUST CSF v8.1	ISO/IEC 27001:2005	ISO/IEC 27001:2013	ITAR	Jericho Forum	Mexico - Federal Law on Protection of Personal Data Held by Private Parties	NERC CIP	NIST SP800-53 R3	NIST SP800-53 R3 Appendix J	NZISM	NZISM v2.5	ODCA UM: PA R2.0: PA ID	PA link level	PCI DSS v2.0	PCI DSS v3.0	PCI DSS v3.2	Shared Assessments 2017 AUP
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (API's) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC) security?	X				S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	CC7.1	.4	G.16.1, I.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-04		COBIT 4.1 AI2.4	APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02	312.8 and 312.10	Application Services > Development Process > Software Quality Assurance	shared	x	Domain 10	N.03.01. (e)	Article: 27 (3)	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14	NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-4 NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1)		1.2.6	45 CFR 164.312(e)(2)(i)	10.b;10.c;10.e	A.15.5.6 A.11.6.1 A.12.2.1 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	A9.4.2 A9.4.1, 8.1*partial, A14.2.1, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2		Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11		CIP-007-3: R5.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22	AR-7 The organization designs information systems to support privacy by automating privacy controls.	14.5 14.6	4.3.8.C.01. 14.4.4.C.01. 14.4.5.C.01. 14.4.6.C.01. 14.4.6.C.02. 14.4.6.C.03. 14.5.6.C.01. 14.5.7.C.01. 14.5.8.C.01.	PA17 PA31	SGP BSGP	PCI DSS v2.0:6.5	6, 6.5	6, 6.5	L13
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and	X				S3.2a	(S3.2 a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC6.1		C.2.1, C.2.3, C.2.4, C.2.6.1, H.1	10 (B) 11 (A+)	Schedule 1 (Section 5), 4.1 Accountability, Subs. 4.1.3	SA-01			APO09.01 APO09.02 APO09.03 APO13.01 BAI02 DSS05	312.3, 312.8 and 312.10	BOSS > Legal Services > Contracts	shared	x	Domain 10		Article 17 (1), (2)	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6		1.2.2 1.2.6 6.2.1 6.2.2		05.j	4.6.2.1 4.6.2.2 4.11.1.1	A9.1.1.		Commandment #6 Commandment #7 Commandment #8			CA-1 CA-2 CA-5 CA-6	AP-1 The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable	9.2	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01.				4.1.1, 4.2, 4.3	4.1.1, 4.2, 4.3	L.3 P.4 P.5 A.8
		AIS-02.2		are all requirements and trust levels for customers' access defined and documented?		X																																										
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X				S3.4	(S3.2.0) The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. (S3.3.0) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (S3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies. (S3.5.0) There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	PI1.2 PI1.3 PI1.5	.4	G.16.1, I.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-05			DSS06.02 DSS06.04	312.8 and 312.10	Application Services > Programming Interfaces > Input Validation	shared	x	Domain 10			NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1) NIST SP 800-53 R3 SI-9 NIST SP 800-53 R3 SI-10 NIST SP 800-53 R3 SI-11		1.2.6	45 CFR 164.312 (c)(1) (New) 45 CFR 164.312 (c)(2)(New) 45 CFR 164.312(e)(2)(i) New)	10.b;10.e	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.6.1 A.15.2.1	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4		Commandment #1 Commandment #9 Commandment #11		CIP-003-3: R4.2	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9	AR-7 The organization designs information systems to support privacy by automating privacy controls.	14.5 14.6	14.4.4.C.01. 14.4.5.C.01. 14.4.6.C.01. 14.4.6.C.02. 14.4.6.C.03. 14.5.6.C.01. 14.5.7.C.01. 14.5.8.C.01. 20.3.13.C.01. 20.3.13.C.02.	PA25	GP	PCI DSS v2.0:6.3.1 PCI DSS v2.0:6.3.2	6.3.1 6.3.2	6.3,6.5.3.2	N.4
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULTICAST, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?		X				(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC6.6	B.1	G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1	6 (B) 26 (A+)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-03	1.1.1;2.1;3.1;4.1;5.1;6.2-7.1;8.1-12.1;11.1;13.2;1.2;4.2;7.2;8.3.1-3.2;3.2.3;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11.1;3.12.1-13;2.14	COBIT 4.1 DS5.11	APO09.01 APO09.02 APO09.03 APO13.01 DSS05.02 DSS06.06 MEA03.01 MEA03.02	312.8 and 312.10	BOSS > Data Governance > Rules for Information Leakage Prevention	shared	x	Domain 10	N.02. (b) N.04.03. (a)	Article 17 (1), (2),(3), (4)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-8	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-8		1.1.0 1.2.2 1.2.6 4.2.3 5.2.1 7.3.2 7.2.1 7.2.2 7.2.3 7.2.4 8.2.1 8.2.2 8.2.3 8.2.5 9.2.1		01.;t;09.x	A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4		All			AC-1 AC-4 SC-1 SC-16	AR-7 The organization designs information systems to support privacy by automating privacy controls.	16.5 16.8 17.4	17.5.5.C.01. 17.5.6.C.01. 17.5.6.C.02. 17.5.7.C.01. 17.5.7.C.02. 17.5.7.C.03. 17.5.8.C.01. 17.5.9.C.01. 17.8.10.C.01. 17.8.10.C.02. 17.8.11.C.01. 17.8.12.C.01. 17.8.13.C.01. 17.8.14.C.01. 17.8.15.C.01. 17.8.16.C.01. 17.8.17.C.01. 18.3.7.C.01. 18.3.8.C.01. 18.3.8.C.02. 18.3.9.C.01. 18.3.10.C.01. 18.3.10.C.02. 18.3.11.C.01. 18.3.11.C.02. 18.3.12.C.01. 18.3.12.C.02. 18.3.13.C.01. 10.3.9.C.01.	PA20 PA25 PA29	GP P SGP	PCI DSS v2.0:2.3 PCI DSS v2.0:3.4.1, PCI DSS v2.0:4.1 PCI DSS v2.0:4.1.1 PCI DSS v2.0:6.1 PCI DSS v2.0:6.3.2a PCI DSS v2.0:6.5c PCI DSS v2.0:8.3 PCI DSS v2.0:10.5.5 PCI DSS v2.0:11.5	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c, 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8 10.5.5, 10.8 11.5, 11.6	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2 6.5b; 7.1; 7.2; 7.3; 8.1; 8.2; 8.3; 8.3.1;8.3.2; 8.4; 8.5; 8.6; 8.7; 8.8 10.5.5; 10.9 11.5; 11.6	B.1
Audit Assurance & Compliance *Audit Planning*	AAC-02	AAC-02.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, GACK's Cloud Computing Management Audit/Assurance Program, etc.)?	X				S4.1.0 S4.2.0	(S4.1.0) The entity's system security is periodically reviewed and compared with the defined system security policies. (S4.2.0) There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	CC4.1		L.1, L.2, L.7, L.9, L.11	58 (B)		CO-01		COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	APO12.04 APO12.05 APO12.06 MEA02.01 MEA02.02	Title 16 Part 312	BOSS > Compliance > Audit Planning	shared	x	Domain 2, 4	N.01. (d)		NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2) NIST SP 800-53 R3 PL-6		10.2.5	45 CFR 164.312(b)	06.j	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	Clauses 4.2(a), 4.2(b), 5.1(g), 5.1(f), 6.2(e), 9.1, 9.1(a), 9.2,		Commandment #1 Commandment #2 Commandment #3			CA-2 CA-7 PL-6	AR-4 Privacy Auditing and Monitoring. To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting	5.1, 5.3, 5.4	4.2.10.C.01. 4.2.11.C.01. 4.2.12.C.01. 4.5.17.C.01. 4.5.18.C.01. 4.5.18.C.02. 4.5.18.C.03. 4.3.7.C.01. 4.3.8.C.01.	PA15	SGP	PCI DSS v2.0:2.1,2.b			A.1 A.2
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.2	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and that the results of these tests are available to tenants at their request?		X			S4.1.0 S4.2.0	(S4.1.0) The entity's system security is periodically reviewed and compared with the defined system security policies. (S4.2.0) There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	CC4.1		L.2, L.4, L.7, L.9, L.11	58 (B) 59 (B) 76 (B) 77 (B)		CO-02		COBIT 4.1 DS5.5, ME3.5, ME 3.1 PO 9.6	APO12.04 APO12.05 APO12.06 MEA02.07 MEA02.08 MEA03.01	Title 16 Part 312	BOSS > Compliance > Independent Audits	shared	x	Domain 2, 4	N.01. (e) N.07.01. (m) N.07.01. (n)		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (5) NIST SP 800-53 R3 RA-5 (8) NIST SP 800-53 R3 RA-5 (9)		1.2.5 1.2.7 6.2.1 8.2.7 10.2.3 10.2.5	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	05.h;06.i;06.j	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1		Commandment #1 Commandment #2 Commandment #3	Chapter VI, Section 1 Article 39, I. and VIII. Chapter 8 Article 59	CIP-003-3: R1.3 - R4.3 CIP-004-3: R4 - R4.2 CIP-005-3a: R1 - R1.1 - R1.2	CA-1 CA-2 CA-6 RA-5	AR-4. Privacy Auditing and Monitoring. These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems.	L1		PCI DSS v2.0:11.2 PCI DSS v2.0:11.3 PCI DSS v2.0:11.4 PCI DSS v2.0 12.1.2.b	11.2 11.3 11.4.6 11.2.1, 11.2.2, 11.2.3, 11.3.1, 11.3.2, 12.1.2.b, 12.8.4	11.2 11.3 11.4.6 11.2.1; 11.2.2; 11.2.3; 11.3.1; 11.3.2; 11.3.3; 11.3.4; 12.8.4	L.2
		AAC-02.3		Do you conduct network penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and the results thereof?	X																																									
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and the results thereof?	X																																									
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and the results thereof?		X																																								
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?		X																																								
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?		X																																								
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?		X																																								
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another	X						CC3.1							2.8.3.7	COBIT 4.1 ME 3.1	APO12.01 APO12.02 APO12.03 MEA03.01	312,4	BOSS > Compliance > Information System Regulatory Mapping	shared	x	Domain 2, 4									06.a	ISO/IEC 27001:2005 Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.1 Clause 5.2.1 a - f Clause 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3 A.15.1.4 A.15.1.6	Clauses 4.2(b), 4.4, 5.2(c), 5.3(abc), 6.1.2, 6.1.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3 9.2(g), 9.3, 9.3(b), 9.3(f), 10.2, A.8.2.1,							1.2 3.2 3.3 5.2	1.2.13.C.01. 1.2.13.C.02. 2.2.5.1.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01. 3.3.4.C.01. 3.3.4.C.02. 3.3.4.C.03. 3.3.4.C.04. 3.3.4.C.05. 3.3.5.C.01. 3.3.5.C.02. 3.3.6.C.01. 3.3.6.C.02. 3.3.6.C.03. 3.3.6.C.04.			PCI DSS v2.0:3.1.1 PCI DSS v2.0:3.1	3.3	3.3	L.3
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X													2.8.3.7																												
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X													2.8.3.7																												
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory	X													2.8.3.7																												
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established,	Do you provide tenants with geographically resilient hosting options?	X				A3.1.0 A3.3.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments, and (2) assess the risks associated with the identified threats.	CC3.1 A1.2 A1.3		K.1.2.3, K.1.2.4, K.1.2.5, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15			RS-03			DSS04.01 DSS04.02 DSS04.03 DSS04.05		BOSS > Operational Risk Management > Business Continuity	provider	x	Domain 7, 8	N.07.01. (a) N.07. (b) N.07. (c)	Article 17 (1), (2)	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-10	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-10			45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C)	12.d	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	Clause 5.1(h) A.17.1.2 A.17.1.2		Commandment #1 Commandment #2 Commandment #3			CP-1 CP-2 CP-3 CP-4 CP-6 CP-7	UL-2 INFORMATION SHARING WITH THIRD PARTIES - a. Shares personally identifiable information (PII) externally, only for the	6.4	6.4.4.C.01. 6.4.5.C.01. 6.4.6.C.01. 6.4.7.C.01.			PCI DSS v2.0:12.5.1 PCI DSS v2.0:12.5.3 PCI DSS v2.0:12.9.4 PCI DSS v2.0:12.9.6	12.9.1 12.9.3 12.9.4 12.9.6	4.1
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?		X																																								
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant)	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X				A3.5.0	(A3.3) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	A1.2		K.1.3, K.1.4.3, K.1.4.6, K.1.4.7, K.1.4.8, K.1.4.9, K.1.4.10, K.1.4.11, K.1.4.12	52 (B) 55 (A+)		RS-04			DSS04.04		BOSS > Operational Risk Management > Business Continuity	provider	x	Domain 7, 8	N.07.01. (b) N.07.01. (j) N.07.01. (l)		NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1)			45 CFR 164.308 (a)(7)(ii)(D)	12.e	A.14.1.5	A17.1.1		Commandment #1 Commandment #2 Commandment #3			CP-2 CP-3 CP-4		6.4 5.2(time limit) 6.3(whenever change occurs)	5.4.5.C.01. 5.4.5.C.02. 5.4.5.C.03. 4.4.4.C.01. 4.4.5.C.01. 4.4.5.C.02. 4.4.5.C.03. 4.4.5.C.04. 4.4.6.C.01. 4.4.7.C.01. 4.4.7.C.02. 4.4.8.C.01.	PA15	SGP	PCI DSS v2.0:12.9.2	12.9.2, 12.10.2	12.10.2	K.6
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications,	Do you provide tenants with documentation showing the transport route of your data?	X				A3.2.0 A3.4.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A3.4.0) Procedures exist to protect against unauthorized access to system resource.	A1.1 A1.2 A1.3	F.1	F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12	9 (B) 10 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3				DSS01.03 DSS01.04 DSS01.05 DSS04.03	312.8 and 312.10	Infra Services > Facility Security > Environmental Risk Management	provider	x	Domain 7, 8	N.08. (a) N.09. (c) N.09. (f) N.09. (g)	Article 17 (1), (2)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)				08.h;08.i	A.9.2.2 A.9.2.3	A11.2.2, A11.2.3		Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #9 Commandment #11			PE-1 PE-4 PE-13		10.1 10.2 10.3 10.4 10.5 10.6	10.1.37.C.01. 10.1.37.C.02. 10.1.38.C.01. 10.1.38.C.02. 10.1.38.C.03. 10.1.38.C.04. 10.1.39.C.01. 10.1.39.C.02.	PA15	SGP		4.1, 4.1.1, 9.1, 9.2	4.1, 4.1.1, 9.1, 9.2	F.1
Business Continuity Management & Operational Resilience *Documentation*	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?		X			S3.11.0 A.2.1.0	(S3.11.0) Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities. (A.2.1.0) The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	CC1.3 CC1.4 CC2.1		G.1.1	56 (B) 57 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	CP-02		COBIT 4.1 DS 9, DS 13.1	BAI08 BAI10 DSS01.01	312.8 and 312.10	BRM > Policies and Standards > Job Aid Guidelines	shared	x	Domain 7, 8		Article 17	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-9 (1) NIST SP 800-53 R3 CP-9 (3) NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 CP-10 (3) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)		1.2.6		09.a;09.r	Clause 4.3.3 A.10.7.4	Clause 9.2(g)		Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11		CIP-005-3a: R1.3 CIP-007-3: R9	CP-9 CP-10 SA-5 SA-10 SA-11		10.5 13.5 17.1	10.5.4.C.01. 10.5.5.C.01. 10.5.6.C.01. 10.5.6.C.02. 10.5.7.C.01. 10.5.8.C.01. 10.5.8.C.02. 10.5.9.C.01. 10.5.9.C.02. 10.5.10.C.01. 10.5.10.C.02. 10.5.11.C.01. 13.6.5.C.01. 13.6.6.C.01. 13.6.7.C.01. 13.6.8.C.01. 13.6.9.C.01. 13.6.9.C.02. 18.1.8.C.01. 18.1.8.C.02. 18.1.8.C.03. 18.1.8.C.04. 18.1.8.C.05. 18.1.9.C.01. 18.1.9.C.02. 18.1.9.C.03. 18.1.9.C.04. 18.1.10.C.01.			PCI DSS v2.0:12.1 PCI DSS v2.0:12.2 PCI DSS v2.0:12.3 PCI DSS v2.0:12.4	1.1

| | | |

		DG-01.3	sensitivity, and criticality to the organization.	Do you have a capability to use system geographic location as an authentication factor?		X				data are classified in accordance with the defined confidentiality and related security policies.						2.B.3.7		BA09.02 BA09.03 DSS04.07 DSS05.04 DSS06.06																																			
		DG-01.4		Can you provide the physical location/geography of storage of a tenant's	X												2.B.3.7																																			
		DG-01.5		Can you provide the physical location/geography of storage of a tenant's	X												2.B.3.7																																			
		DG-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		X											2.B.3.7																																			
		DG-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X												2.B.3.7																																			
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?		X													APO01.06 APO03.01 APO03.02 APO09.01 APO09.03 BAI08.03 BAI09.01 BAI10.01 BAI10.02 BAI10.03 BAI10.04 BAI10.05		BOSS > Data Governance > Handling / Labeling / Security Policy			Domain 5													01.m		Clause 4.2 5.2, 7.5, 8.1						Relearch.							1.1.3 12.3.3	1.1.3 12.3.3; 12.3.10	L.4 P.1
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	X																																															
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X				S3.6	S3.6) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.	CCS.7 PI1.5	G.4 G.11 G.16 G.18 L.3 L.4	G.19.1.1, G.19.1.2, G.19.1.3, G.10.8, G.9.11, G.14, G.15.1		Schedule 1 (Section 51, 4.7 - Safeguards, Subsec. 4.7.3	S-28	2.B.3.7	COBIT 4.1 DS 5.10 5.11	APO01.06 APO03.01 APO03.02 APO08.01 APO13.01 DSS05 DSS06	312.8 and 312.10	BRM > Cryptographic Services > Data in Transit Encryption	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-1	NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1)		3.2.4 4.2.3 7.1.2 7.2.1 7.2.2 8.2.1 8.2.5	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	09.x,09.y	4.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4		Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11				AC-14 AC-21 AC-22 IA-8 AU-10 SC-4 SC-8 SC-9		TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS			PA25 PA21 PA5	GP GP BSGP	PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2	2.1.1 3.1 4.1 4.1.1 4.2	2.1.1;3.1;4.1;4.1.1;4.2	D.1 D.6 P.1
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X				S3.8.a-e	(S3.8.a-e) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.																																								
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?		X			S3.2.a	S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CCS.1	G.13	D.2.2			DG-03		COBIT 4.1 PO 2.3, DS 11.6	APO01.06 APO03.02 APO08.01 APO09.03 APO13.01 BAI09.01	312.2	BOSS > Data Governance > Handling / Labeling / Security Policy	shared	x	Domain 5	G.03.05. (b)	Article 22 Article 23	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-18 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-16 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-3 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SC-9	99.31.(a)(1)(ii)	1.1.2 5.1.0 7.1.2 8.1.0 8.2.5 8.3.6		07.e	4.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1		Commandment #8 Commandment #9 Commandment #10	Chapter II Article 8, 9, 11, 12, 14, 18, 19, 20, 21	CIP-003-3: R4 - R4.1	AC-16 MP-1 MP-3 PE-16 SI-12 SC-9		DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and	11.1	13.1.7.C.01. 13.1.8.C.01. 13.1.8.C.02. 13.1.8.C.03. 13.1.8.C.04. 13.1.8.C.05.			PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.10	9.5, 9.5.1 9.6 9.7 9.8 9.9	9.5; 9.5.1 9.6 9.7 9.8 9.9	D.2
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?					S3.5.0 S3.4.0 C3.21.0	(C3.5.0) The system processes information that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources. (C3.21.0) Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.	CI-3 CCS.6 C1.1		I-2.18			DG-06			APO01.06 BAI01.03 BAI03.07 BAI07.04		BRM > Policies and Standards > Technical Standard (Data Management Security Standard)	shared	x	Domain 5	G.03. (d)		NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)			1.2.6	45 CFR 164.308(a)(4)(ii)(B)	10.j	4.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	A.8.1.3 A.12.1.4 A.14.1.1 8.1* (partial) A.14.2.2.		Commandment #9 Commandment #10 Commandment #11		CIP-003-3: R6	SA-11 CM-04		DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and Research. SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	12.8	12.4.4.C.02 14.4.4.C.01 19.1.21.C.03 20.1.5.C.01 20.1.5.C.02 20.1.6.C.03. 20.1.6.C.02. 20.1.7.C.01 20.1.8.C.01. 20.1.9.C.01. 20.1.9.C.02. 20.1.10.C.03. 20.1.11.C.03. 20.1.12.C.03.			PCI DSS v2.0 6.4.3	6.4.3	6.4.3	I.11
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?		X			S2.2.0 S2.3.0 S3.8.0	(S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	CC2.3 CC5.1		C.2.5.1, C.2.5.2, D-1.3, L.7		Schedule 1 (Section 51 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.1.3	DG-01	2.B.3.7	COBIT 4.1 DS5.1, PO 2.3	APO01.06 APO03.02 APO09.01 APO13.03	312.4	BOSS > Data Governance > Data Ownership / Stewardship	shared	x	Domain 5		Article 4	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2		6.2.1	45 CFR 164.308 (a)(2)	07.b	4.6.1.3 4.7.1.2 A.15.1.4	4.6.1.1 A.8.1.2 A.18.1.4		Commandment #6 Commandment #10	Chapter IV Article 30	CIP-007-3: R1.1 - R1.2	CA-2 PM-5 PS-2 RA-2 SA-2		AP-1 AUTHORITY TO COLLECT. AP-2 PURPOSE SPECIFICATION.	1.4	3.4.8.C.01. 3.4.8.C.02. 3.4.9.C.01. 3.4.10C.01. 3.4.10.C.02.				3.7 12.5.5 12.10.4	3.7 12.5.5 12.10.4	D.1
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined	X				S3.5.0 S3.4.0	(S3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.	CI-3 CCS.6		C.2.5.10, D.2.2.11, D.2.2.14,	I7 (B)	Schedule 1 (Section 51 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.7.5 and 4.5.3	DG-05	2.B.3.7 2.B.3.7	COBIT 4.1 DS 11.4	APO01.06 APO13.01 BAI09.03 DSS01.01	312.3	BOSS > Data Governance > Secure Disposal of Data	shared	x	Domain 5	G.03. (h)	Article 16 Article 17	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 PE-1	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 MP-6 (4) NIST SP 800-53 R3 PE-1		5.1.0 5.2.3	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	08.l,09.p	4.9.2.6 A.10.7.2	A.11.2.7 A.8.3.2		Commandment #11		CIP-007-3: R7 - R7.1 - R7.2 R7.3	MP-6 PE-1		DM-2 DATA RETENTION AND DISPOSAL	13.4 13.5	13.1.7.C.01 13.5.5.C.01. 13.5.6.C.01. 13.5.6.C.02. 13.5.7.C.01. 13.5.8.C.01. 13.5.9.C.01. 13.5.9.C.02. 13.5.9.C.03. 13.5.10.C.09.			PCI DSS v2.0 3.1.1 PCI DSS v2.0 9.10 PCI DSS v2.0 9.10.1 PCI DSS v2.0 9.10.2 PCI DSS v2.0 3.1	3.1.1 9.8, 9.8.1, 9.8.2, 3.1	3.1 9.8.1; 9.8.2; 3.1	D.8
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and compliance	Do you maintain a complete inventory of all of your critical assets that includes	X				S3.1.0	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	CCS.1				Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.3	PS-08			APO01.06 APO03.02 APO08.01 APO09.03 BAI09.01		ITOS > Service Support > Configuration Management - Physical Inventory	provider	x	Domain 8		Article 17				45 CFR 164.310 (d)(2)(iii)	07.a,07.b	4.7.1.1 A.7.1.2	Annex A.8					NIST SP800-53 R3 CM-8			12.3	12.3.4.C.01. 12.3.5.C.01. 12.3.5.C.02. 12.3.6.C.01. 12.3.7.C.01.		PA4 PA8 PA37 PA38	BSGP BSGP SGP SGP	PCI DSS v2.0 9.9.1 PCI DSS v2.0 12.3.3 PCI DSS v2.0 12.3.4	9.7.1 9.9 9.9.1	9.7.1 9.9 9.9.1; 9.9.2; 9.9.3	D.1
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	X																																															
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	X			Defined by firewall	A1.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CCS.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7.1-8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	I7 (B)	Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.3	PS-03		COBIT 4.1 DS 12.3	APO13.01 DSS01.01 DSS05.05 DSS06.03 DSS06.06	312.8 and 312.10	Infra Services > Facility Security > Controlled Physical Access	provider	x	Domain 8	G.08. (a) G.09. (i)	Article 17	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-8	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1) NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-7 (1) NIST SP 800-53 R3 PE-8 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-17 NIST SP 800-53 R3 PE-18	99.31.a.1.ii	8.2.3		08.a	4.9.1.1	A.11.1.1 A.11.1.2		Commandment #1 Commandment #2 Commandment #3 Commandment #5		CIP-006-3c: R1.2 - R1.3 - R1.4 - R1.5 - R1.6.1 - R2 - R2.2	PE-2 PE-3 PE-6 PE-7 PE-8 PE-18			8.1 8.2	8.1.9.C.01. 8.1.10C.01. 8.1.11C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01.		PA4	BSGP	PCI DSS v2.0 9.1	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	F.2
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X				S3.2.a	S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CCS.1	D.1	D.1.1, D.1.3		Schedule 1 (Section 51, 4.7 - Safeguards, Subsec. 4.7.3	SA-13		COBIT 4.1 DS5.7	APO13.01 DSS05.02 DSS05.03	312.3, 312.8 and 312.10	> >			Domain 8	G.05. (a)		NIST SP 800-53 R3 IA-3 NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-4 (4)					01.x	A.11.4.3			Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #8			IA-3 IA-4					PA22 PA33	GP SGP			0
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)?				X	S3.2.f C3.9.0	S3.2.f) f. Restriction of access to offline storage, backup data, systems, and media. (C3.9.0) Procedures exist to restrict physical access to the defined system including, but not limited to facilities, backup media, and other system components such as firewalls, routers, and servers.	CCS.1 CCS.5		F.2.18, F.2.19,		Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.5	PS-06			EDM05.02 APO01.02 APO03.02 BAI02.03 BAI02.04 BAI03.09 BAI06.01	312.8 and 312.10	BRM > Facility Security > Asset Handling	provider	x	Domain 8	G.08. (a) G.09. (j)	Article 17	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-17 (1) NIST SP 800-53 R3 AC-17 (2) NIST SP 800-53 R3 AC-17 (3) NIST SP 800-53 R3 AC-17 (4) NIST SP 800-53 R3 AC-17 (5) NIST SP 800-53 R3 AC-17 (7) NIST SP 800-53 R3 AC-17 (8) NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-17			45 CFR 164.310 (d)(1) (New)	08.k,08.m	4.9.2.7 A.10.1.2	A.11.2.6 A.11.2.7		Commandment #4 Commandment #5 Commandment #11			AC-17 MA-1 PE-1 PE-16 PE-17			12.5 15.1	12.5.5.C.01 12.5.3.C.02. 12.5.4.C.01. 12.5.4.C.02. 12.5.4.C.03. 12.5.4.C.04. 12.5.5.C.01. 12.5.6.C.01. 12.5.6.C.02. 21.1.8.C.01. 21.1.8.C.02. 21.1.8.C.03. 21.1.9.C.01. 21.1.9.C.02.		PA4	BSGP	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9	9.6.3	9.6.3	D.1
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a waiver	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	X				S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CCS.6	D.1	D.1.1, D.2.1, D.2.2,		Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.5	PS-07			APO09.03 APO10.04 APO10.05 APO13.01 DSS01.02	312.8 and 312.10	BOSS > Data Governance > Secure Disposal of Data	provider	x	Domain 8	G.05. (a) G.05. (b) G.05. (c)	Article 17	NIST SP 800-53 R3 CM-8	NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 CM-8 (1) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 SC-30			45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) (New) 45 CFR 164.310 (d)(2)(i) (New)	08.x	4.9.2.5 4.9.2.6	A.8.1.1 A.8.1.2		Commandment #6 Commandment #7 Commandment #8			CM-8			12.6	12.6.4.C.01. 12.6.4.C.02. 12.6.5.C.01. 12.6.5.C.02. 12.6.5.C.03. 12.6.5.C.04. 12.6.5.C.05. 12.6.6.C.01. 12.6.6.C.02.		PA4	BSGP	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 9.10	9.8, 9.8.1, 9.8.2 12.3	9.8; 9.8.1; 9.8.2 12.3	D.8
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and	X				A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CCS.5	H.6	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7.1-8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	I7 (B)	Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.3	PS-04		COBIT 4.1 DS5.7, DS 12.1, DS 12.4, DS 4.9	APO13.01 DSS01.04 DSS01.05 DSS04.01 DSS04.03	312.8 and 312.10	BRM > Policies and Standards > Information Security Policies (Facility Security Policy)	provider	x	Domain 8	G.08. (a) G.09. (i)	Article 17	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-4 NIST SP 800-53 R3 PE-5 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1)	99.31.a.1.ii	8.2.1 8.2.2 8.2.3	45 CFR 164.310 (a)(1) 45 CFR 164.310 (a)(2)(ii) 45 CFR 164.308(a)(3)(ii)(A) (New)	08.c	4.5.1.1 4.9.1.3 A.9.1.5	A.11.1.1 A.11.1.2		Commandment #1 Commandment #2 Commandment #3 Commandment #5		CIP-006-3c: R1.2 - R1.3 - R1.4 - R2 - R2.2	PE-2 PE-3 PE-4 PE-5 PE-6			4.2 8.1	5.2.3.E.01. 5.2.3.E.02. 8.1.9.C.01. 8.1.10C.01. 8.1.11C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01.		PA4	BSGP	PCI DSS v2.0 9.1 PCI DSS v2.0 9.2 PCI DSS v2.0 9.3 PCI DSS v2.0 9.4	9.1 9.1.1 9.1.2 9.2 9.3 9.4	9.1 9.1.1 9.1.2 9.2 9.3 9.4	F.3
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X																																														
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?		X			A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CCS.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7.1-8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	I7 (B)	Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.3	PS-04		DS 12.2, DS 12.3	APO13.01 APO13.02 DSS05.05	312.8 and 312.10	BRM > Policies and Standards > Information Security Policy (Facility Security Policy)	provider	x	Domain 8	G.08. (a) G.09. (i)	Article 17	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-7 (1) NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-18	99.31.a.1.ii	8.2.3		08.b	4.9.1.1 A.9.1.2	A.11.1.6		Commandment #1 Commandment #2 Commandment #3 Commandment #5		CIP-006-3c: R1.2 - R1.3 - R1.4	PE-7 PE-16 PE-18			8.2 8.3	8.1.9.C.01. 8.1.10C.01. 8.1.11C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01.		PA4	BSGP	PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.2	9.1 9.1.1 9.1.3	9.1;9.1;9.1.3	F.4
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X				A1.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CCS.5	G.21	F.2.18		Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.3	PS-05		COBIT 4.1 DS 12.3	APO13.01 APO13.02 DSS05.05 DSS06.05	312.8 and 312.10	BRM > Policies and Standards > Information Security Policy (Facility Security Policy)	provider	x	Domain 8	G.08. (a) G.09. (j)	Article 17	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-2 (1) NIST SP 800-53 R3 PE-16	99.31.a.1.ii	8.2.5 8.2.6		08.f	4.9.1.6	A.11.2.5 8.1* (partial) A.12.1.2		Commandment #6 Commandment #7			MA-1 MA-2 PE-16			8.1 8.2 8.3 8.4	8.1.10C.01. 8.1.10C.02. 8.1.11.C.01. 8.1.11.C.02. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02.		PA4	BSGP		9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	F.4
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X				A1.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CCS.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7.1-8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	I7 (B) I2 (B)	Schedule 1 (Section 51, 4.7 Safeguards, Subsec. 4.7.3	PS-02			APO13.01 APO13.02 DSS05.04 DSS05.05 DSS06.03	312.8 and 312.10	Infra Services > Facility Security >	provider	x	Domain 8	G.08. (a) G.09. (i)	Article 17	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST S

| | | |

| | | |

| | | |

| | | |

| | | |

| | | |