Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	監査計画や活動、データ複製やアクセス制限、データ範囲(boundary)制限を中心とした運用活動は、業務プロセスの中断リスクを最小限に抑えるよう設計されなければならない。監査活動は、利害関係者の事前合意に基づき、計画されなければならない。	個人情報を取扱う場合、金融情報を扱う場合、委託先の管理監督義務は発注者側にある。	X	X	X	X	X	X	X	X	X	X	X	X	ME 2.1 ME 2.2 PO 9.5 PO 9.6	45 CFR 164.312(b)	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	CA-2 CA-7 PL-6	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PL-6	2.1.2.b	L.1, L.2, L.7, L.9, L.11		10.2.5	Commandment #1 Commandment #2 Commandment #3	
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	組織が、方針や手順、規格、規制の諸要求事項(内部/外部監査、認証、脆弱性及びペネトレーションテストなど)に準拠していることを保証するために、独立したレビューや評価が少なくとも年1回、もしくはあらかじめ定められた間隔で実施されるものとする。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.5 ME2.5 ME 3.1 PO 9.6	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	CA-1 CA-2 CA-6 RA-5	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-6 NIST SP800-53 R3 RA-5 NIST SP800-53 R3 RA-5 (1) NIST SP800-53 R3 RA-5 (2) NIST SP800-53 R3 RA-5 (3) NIST SP800-53 R3 RA-5 (9) NIST SP800-53 R3 RA-5 (6)	11.2 11.3 6.6 12.1.2.b	L.2, L.4, L.7, L.9, L.11		1.2.5 1.2.7 4.2.1 8.2.7 10.2.3 10.2.5	Commandment #1 Commandment #2 Commandment #3	CIP-003-3 - R1.3 - R4.3 CIP-004-3 R4 - R4.2 CIP-005-3a - R1 - R1.1 - R1.2
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	サービスプロバイダは、契約に含まれる情報セキュリティや機密性、サービス定義、SLA(delivery level agreement)を順守しなければならない。SLAの順守状況を管理・維持するために、第三者の報告、記録、サービスは、定期的に監査及びレビューを受けなければならない。		X	X	X	X	X	X	X	X	X	X	X		ME 2.6 DS 2.1 DS 2.4	45 CFR 164.308(b)(1) 45 CFR 164.308 (b)(4)	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	CA-3 SA-9 SA-12 SC-7	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1) NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	2.4 12.8.2 12.8.3 12.8.4 Appendix A	C.2.4,C.2.6, G.4.1, G.4.2, L.2, L.4, L.7, L.11	C.2	1.2.11 4.2.3 7.2.4 10.2.3 10.2.4	Commandment #1 Commandment #2 Commandment #3	
Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact.	関係当局との連絡窓口は、事業や顧客の要求事項、及び法律、規制、契約上の要求事項に沿って、維持しなければならない。適切かつ適法な連絡先の設置を容易にするために、データ、オブジェクト、アプリケーション、インフラ、ハードウェアが立法分野及び司法に割り当てられてもよい。		X	X	X	X	X	X	X	X	X	X	X	X	ME 3.1		A.6.1.6 A.6.1.7	AT-5 IR-6 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-6 (1) NIST SP800-53 R3 SI-5	11.1.e 12.5.3 12.9	L1		1.2.7 10.1.1 10.2.4	Commandment #1 Commandment #2 Commandment #3	CIP-001-1a R3 - R4
Compliance - Information System Regulatory Mapping	CO-05	Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure and hardware. Each element may be assigned a legislative domain and jurisdiction to facilitate proper compliance mapping.	情報システムの全構成要素について、法令、規制及び契約上の要求事項が定義されなければならない。既存の規制を満たし、また新しい規制に適合するための組織の取り組みは、情報システムの各構成要素について明示的に定義され、文書化され、更新されなければならない。情報システムの構成要素には、データ、オブジェクト、アプリケーション、インフラ、ハードウェアを含んでもよい。各構成要素は、法的要求事項の順守を促進するために、立法分野及び司法に割り当てられてもよい。		X	X	X	X	X	X	X	X	X	X	X	X	ME 3.1		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 4.3.3 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	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 RA-2 SA-1 SA-6 SC-1 SC-13 SI-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CP-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 RA-1 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SI-1	3.1.1 3.1	L.1, L.2, L.4, L.7, L.9		1.2.2 1.2.4 1.2.6 1.2.11 3.2.4 5.2.1	Commandment #1 Commandment #2 Commandment #3	
Compliance - Intellectual Property	CO-06	Policy, process and procedure shall be established and implemented to safeguard intellectual property and the use of proprietary software within the legislative jurisdiction and contractual constraints governing the organization.	知的財産権や権利関係のあるソフトウェア製品の利用を保護するために、組織に適用される法律及び契約に沿って、方針、手続き、手順が確立され、施行されなければならない。						X	X	X	X	X	X	X	X			Clause 4.2.1 A.6.1.5 A.7.1.3 A.10.8.2 A.12.4.3 A.15.1.2	SA-6 SA-7 PM-5	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5		L.4			Commandment #1 Commandment #2 Commandment #3	
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	全情報について、管理責任者が指名されなければならない。管理責任者の責任は、定義され、文書化され、通知されなければならない。				X	X	X	X	X	X	X	X	X		DS5.1 PO 2.3	45 CFR 164.308 (a)(2)	A.6.1.3 A.7.1.2 A.15.1.4	CA-2 PM-5 PS-2 RA-2 SA-2	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-2		C.2.5.1, C.2.5.2, D.1.3, L.7		6.2.1	Commandment #6 Commandment #10	CIP-007-3 - R1.1 - R1.2
Data Governance - Classification	DG-02	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.	データや、データを含むオブジェクトは、認可されていない開示や誤用を防ぐために、データタイプ、出身地や居住地の司法権、法的、契約的制約、組織や第三者にとっての価値や機密性や重要性に基づき、分類されなければならない。				X	X	X	X	X	X	X	X	X	X	PO 2.3 DS 11.6		A.7.2.1	RA-2 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	9.7.1 9.10 12.3	D.1.3, D.2.2		1.2.3 1.2.6 4.1.2 8.2.1 8.2.5 8.2.6	Commandment #9	CIP-003-3 - R4 - R5
Data Governance - Handling / Labeling / Security Policy	DG-03	Polices and procedures shall be established for labeling, handling and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that acts as aggregate containers for data.	データや、データを含むオブジェクトのラベリング、取扱、セキュリティのための方針、手順が確立されなければならない。組織が採用したラベル体系は、データの集合体としてのオブジェクトに対して適用されなければならない。				X	X	X	X	X	X	X	X	X	X	PO 2.3 DS 11.6		A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	AC-16 MP-1 MP-3 PE-16 SI-12 SC-9	NIST SP800-53 R3 AC-16 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1)	9.5 9.6 9.7.1 9.7.2 9.10	D.2.2	G.13	1.1.2 5.1.0 7.1.2 8.1.0 8.2.5 8.2.6	Commandment #8 Commandment #9 Commandment #10	CIP-003-3 - R4 - R4.1

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Data Governance - Retention Policy	DG-04	(v1.0) Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals. (v1.1) Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of backups must be implemented at planned intervals.	データ保管のための方針、手順が確立され、法的、契約的、事業的要求事項を順守するために、バックアップや冗長化のメカニズムが導入されなければならない。バックアップからのリカバリテストは定期的に実施されなければならない。	Control revision v1.1 rationale: Removed the specific reference to tape and disk backup as there are other media types. 他のメディアタイプがあるので、テープとディスクバックアップへの特定の参照を削除しました。			X	X	X	X	X	X	X	X	X	X	DS 4.1 DS 4.2 DS 4.5 DS 4.9 DS 11.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) 45 CFR 164.316(b)(2)(i) (New)	Clause 4.3.3 A.10.5.1 A.10.7.3	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11	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-6 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (3) NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-7 (1) NIST SP800-53 R3 CP-7 (2) NIST SP800-53 R3 CP-7 (3) NIST SP800-53 R3 CP-7 (5) NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 SI-12 NIST SP800-53 R3 AU-11	3.1 3.1.1 3.2 9.9.1 9.5 9.6 10.7	D.2.2.9		5.1.0 5.1.1 5.2.2 8.2.6	Commandment #11	CIP-003-3 - R4.1
Data Governance - Secure Disposal	DG-05	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	あらゆるストレージメディアからデータを完全に消去し、安全に廃棄するための方針、手順、メカニズムが確立され、いかなるフォレンジック手法によってもデータが回復できないようにしなければならない。				X	X	X	X	X	X	X	X	X		DS 11.4	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.9.2.6 A.10.7.2	MP-6 PE-1	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4) NIST SP800-53 R3 PE-1	3.1.1 9.10 9.10.1 9.10.2 3.1	D.2.2.10, D.2.2.11, D.2.2.14,		5.1.0 5.2.3	Commandment #11	CIP-007-3 - R7 - R7.1 - R7.2 R7.3
Data Governance - Non-Production Data	DG-06	Production data shall not be replicated or used in non-production environments.	本番データは、本番環境以外で使われたり、複製されたりしてはならない。					X	X	X		X	X	X	X			45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	SA-11 CM-04	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 CM-04	6.4.3	I.2.18		1.2.6	Commandment #9 Commandment #10 Commandment #11	CIP-003-3 - R6
Data Governance - Information Leakage	DG-07	Security mechanisms shall be implemented to prevent data leakage.	データ漏えいを防ぐために、セキュリティのメカニズムが導入されなければならない。				X	X	X	X	X	X	X	X	X		DS 11.6		A.10.6.2 A.12.5.4	AC-2 AC-3 AC-4 AC-6 AC-11 AU-13 PE-19 SC-28 SA-8 SI-7	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-3 (3) NIST SP800-53 R3 AC-4 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 AU-13 NIST SP800-53 R3 PE-19 NIST SP800-53 R3 SC-28 NIST SP800-53 R3 SC-28 (1) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1)	1.2 6.5.5 11.1 11.2 11.3 11.4 A.1	I.2.18		7.2.1 8.1.0 8.1.1 8.2.1 8.2.2 8.2.5 8.2.6	Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8 Commandment #9 Commandment #10 Commandment #11	
Data Governance - Risk Assessments	DG-08	Risk assessments associated with data governance requirements shall be conducted at planned intervals considering the following: ・Awareness of where sensitive data is stored and transmitted across applications, databases, servers and network infrastructure ・Compliance with defined retention periods and end-of-life disposal requirements ・Data classification and protection from unauthorized use, access, loss, destruction, and falsification	データ管理の要求事項にかかわるリスクアセスメントは、以下を考慮に入れ、定期的に実施されなければならない。 ・機密データがどこに保管され、どのようなアプリケーションやデータベース、サーバ、ネットワークインフラ間でやり取りされているかを認識すること ・所定の保管期間や保管期限満了後の廃棄の要件を順守すること ・データの分類及び認可されていない使用、アクセス、紛失、破壊、偽造からの保護				X	X	X	X	X	X	X	X	X	X	PO 9.1 PO 9.2 PO 9.4 DS 5.7	45 CFR 164.308(a)(1)(ii)(A) 45 CFR 164.308(a)(8)	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3 A.15.1.4	CA-3 RA-2 RA-3 MP-8 PM-9 SI-12	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	12.1 12.1.2	L.4, L.5, L.6, L.7		1.2.4 8.2.1	Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7 Commandment #9 Commandment #10 Commandment #11	
Facility Security - Policy	FS-01	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.	オフィスや部屋、施設、セキュリティエリア内での安全な労働環境を維持するための方針や手順が確立されなければならない。		X						X	X	X	X	X	X	DS5.7 DS 12.1 DS 12.4 DS 4.9	45 CFR 164.310 (a)(1) 45 CFR 164.310 (a)(2)(ii) 45 CFR 164.308(a)(3)(ii)(A) 45 CFR 164.310 (a)(2)(iii) (New)	A.5.1.1 A.9.1.3 A.9.1.5	CA-2 PE-1 PE-6 PE-7 PE-8	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8	9.1 9.2 9.3 9.4	F.1.1, F.1.2 F.1.3, F.1.4, F1.5, F.1.6, F.1.7, F.1.8, F.1.9, F.2.1, F.2.2, F.2.3, F.2.4, F.2.5, F2.6, F.2.7, F.2.8, F.2.9, F.2.10, F.2.11, F.2.12, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18,F.2.19, F.2.20	F.2	8.1.0 8.1.1 8.2.1	Commandment #1 Commandment #2 Commandment #3 Commandment #5	
Facility Security - User Access	FS-02	Physical access to information assets and functions by users and support personnel shall be restricted.	ユーザ及びサポートスタッフによる情報資産や機能への物理的なアクセスは制限されなければならない。		X										X	X		45 CFR 164.310(a)(1) 45 CFR 164.310(a)(2)(ii) 45 CFR 164.310(b) 45 CFR 164.310 (c) (New)	A.9.1.1 A.9.1.2	PE-2 PE-3 PE-4 PE-5 PE-6	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1)	9.1	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.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	H.6	8.2.1 8.2.2 8.2.3	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4 R2 - R2.2
Facility Security - Controlled Access Points	FS-03	Physical security perimeters (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.	機密データや情報システムを保護するため、物理的セキュリティ境界（たとえば、囲い、壁、ガードマン、ゲート、電子的な監視、物理的な認証メカニズム、受付、セキュリティパトロール）を設置しなければならない。		X							X	X	X	X		DS 12.3		A.9.1.1	PE-2 PE-3 PE-6 PE-18	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-18	9.1	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,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	F.2	8.2.3	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4 R1.6 - R1.6.1 - R2 - R2.2
Facility Security - Secure Area Authorization	FS-04	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.	認可された者だけにアクセスを許すことを確実にするために、セキュリティエリアへの入退室は、物理的なアクセス制御メカニズムにより制限され、監視されなければならない。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Physical controls and attestation mechanisms shall be designed to address the requirements of legislative plurality and their results shared with tenants. 物理的な制御と認証システムは複数の法的要件を満たしている事をテナントと確認しておく事。	X							X	X	X	X		DS 12.2 DS 12.3		A.9.1.1 A.9.1.2	PE-2 PE-3 PE-6 PE-7 PE-8 PE-18	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-18	9.1 9.1.1 9.1.2 9.1.3 9.2	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,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	F.2	8.2.3	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4 R1.6 - R1.6.1 - R2 - R2.2
Facility Security - Unauthorized Persons Entry	FS-05	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 facilities to percent unauthorized data corruption, compromise and loss.	サービスエリアなどの出入口、及び許可されていない者が敷地内に立ち入ることもある場所は、監視、管理し、また可能であれば、データの変造、改ざん、紛失を避けるために、データ保管・処理施設から離すこと。	施設の管理・清掃業者、自動販売機のメンテナンス要員等、データへのアクセス権が無い者が立ち入る可能性が有る場合、帯同もしくは監視等を行う事。 特に機密情報がある区画への立入りは、帯同し目視による監視を行う事。 機密情報より機密度の低い情報の場合は、守秘契約を締結し、監視カメラによる録画の元単独での立入りを認める。	X	X	X	X	X	X		X	X	X	X		DS 12.3		A.9.1.6	PE-7 PE-16 PE-18	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18		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,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	F.2	8.2.3	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability								
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Facility Security - Off-Site Authorization	FS-06	Authorization must be obtained prior to relocation or transfer of hardware, software or data to an offsite premises.	ハードウェア、ソフトウェア、またはデータは、事前の許可なく、構外に移転しないこと。	ハード、ソフト、データを別の施設に移転させる場合は、担当者の上席者による承認を得る事 パブリッククラウドの場合、各利用者の承認が必要である。但し、利用約款にて障害対応のみに別施設にハード・ソフト・データを移設する事が書いてある場合は、通知のみで構わない。	X	X	X	X				X	X	X	X			45 CFR 164.310 (d)(1)	A.9.2.7 A.10.1.2	MA-1 MA-2 PE-16	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-2 (1) NIST SP800-53 R3 PE-16	9.8 9.9	F.2.18	G.21		8.2.5 8.2.6	Commandment #6 Commandment #7	
Facility Security - Off-Site Equipment	FS-07	Policies and procedures shall be established for securing and asset management for the use and secure disposal of equipment maintained and used outside the organization's premise.	組織の構外で保管され、使用される装置については、使用や確実な処分に関する資産管理の方針や手続きが確立されなければならない。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Policies and procedures governing asset management shall be established for secure repurposing of equipment and resources prior to tenant assignment or jurisdictional transport. 設備およびリソースの安全な再利用を行うにあたり、テナントへの割り当てまたは管轄変更(移動)が行われる前に、資産管理を統制する方針および手順を定めておく事。	X			X		X	X	X	X	X	X			45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) 45 CFR 164.310 (d)(2)(i)	A.9.2.5 A.9.2.6	AC-17 MA-1 PE-1 PE-16 PE-17	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-17 (1) NIST SP800-53 R3 AC-17 (2) NIST SP800-53 R3 AC-17 (3) NIST SP800-53 R3 AC-17 (4) NIST SP800-53 R3 AC-17 (5) NIST SP800-53 R3 AC-17 (7) NIST SP800-53 R3 AC-17 (8) NIST SP800-53 R3 MA-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-17	9.8 9.9 9.10	F.2.18, F.2.19,				Commandment #4 Commandment #5 Commandment #11	
Facility Security - Asset Management	FS-08	A complete inventory of critical assets shall be maintained with ownership defined and documented.	重要な資産すべてについて、所有者を定義し、文書化した目録を作成し、維持すること。		X	X	X	X	X	X	X	X	X	X	X	X		45 CFR 164.310 (d)(2)(iii)	A.7.1.1 A.7.1.2	CM-8	NIST SP800-53 R3 CM-8 NIST SP800-53 R3 CM-8 (1) NIST SP800-53 R3 CM-8 (3) NIST SP800-53 R3 CM-8 (5)	9.9.1 12.3.3 12.3.4	D.1.1, D.2.1. D.2.2,	D.1			Commandment #6 Commandment #7 Commandment #8	
Human Resources Security - Background Screening	HR-01	Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.	従業員、契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は、関連のある法令、規則及び倫理に従って行うこと。この確認は、アクセスされるデータの分類及び事業の要求事項、受容可能なリスクに応じて行われること。							X	X	X	X	X	X	X	PO 7.6		A.8.1.2	PS-2 PS-3	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	12.7 12.8.3	E.2	E.2	1.2.9	Commandment #2 Commandment #3 Commandment #6 Commandment #9	CIP-004-3 - R2.2
Human Resources Security - Employment Agreements	HR-02	(v1.0) Prior to granting individuals physical or logical access to facilities, systems or data, employees, contractors, third party users and customers shall contractually agree and sign the terms and conditions of their employment or service contract, which must explicitly include the parties responsibility for information security. (v1.1) Prior to granting individuals physical or logical access to facilities, systems or data, employees, contractors, third party users and tenants and/or customers shall contractually agree and sign equivalent terms and conditions regarding information security responsibilities in employment or service contract.	施設やシステム、またはデータへの物理的または論理的アクセスを許可する前に、従業員、契約相手、第三者の利用者及び顧客は、情報セキュリティに関する、これらの者の責任を明示的に定めた雇用契約書もしくはサービス契約書に同意し、署名すること。	Control revision v1.1 rationale: Added "tenant" into scope of control specification. 制御(規制、管理)仕様書の(詳細)の適用範囲に「テナント」を追加。	X	X	X	X	X	X	X	X	X	X	X	X	DS 2.1	45 CFR 164.310(a)(1) 45 CFR 164.308(a)(4)(i)	A.6.1.5 A.8.1.3	PL-4 PS-6 PS-7	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	12.4 12.8.2	E.3.5	C.1	1.2.9 8.2.6	Commandment #6 Commandment #7	
Human Resources - Employment Termination	HR-03	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented and communicated.	雇用の終了もしくは雇用手続きの変更に関する役割及び責任は、明確に割り当て、文書化し、伝達されること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Roles and responsibilities following employment termination or change in employment procedures must follow the terms of the master agreement with the tenant(s). 就業手続きで定められている退職者・異動に伴う職務権限は、テナントとの主契約内の条件と一致(準拠)している事							X	X	X	X	X	X	PO 7.8	45 CFR 164.308 (a)(3)(ii)(C)	A.8.3.1	PS-4 PS-5	NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5		E.6		8.2.2 10.2.5	Commandment #6 Commandment #7	
Information Security - Management Program	IS-01	An Information Security Management Program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	資産やデータを紛失、誤用、許可されていないアクセス、開示、改変、破壊から保護するために、管理的、技術的、物理的保護措置を含む情報セキュリティマネジメントプログラム(ISMP)を作成、文書化し、承認、導入すること。セキュリティプログラムは、以下を取り扱うこと。ただし、事業の特性に関わる限りは、以下のみに限定されるものではない。 ・リスク管理 ・セキュリティ方針 ・情報セキュリティの組織 ・資産管理 ・人的セキュリティ ・物理的、環境的なセキュリティ ・意思伝達(communication)や運用管理 ・アクセス制御 ・情報システムの取得、開発、保守		X	X	X	X	X	X	X	X	X	X	X	X	R2 DS5.2 R2 DS5.5	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR 164.316(b)(1)(i) 45 CFR 164.308(a)(3)(i) (New) 45 CFR 164.306(a) (New)	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	PM-1 PM-2 PM-3 PM-4 PM-5 PM-6 PM-7 PM-8 PM-9 PM-10 PM-11	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	12.1 12.2	A.1, B.1		8.2.1	Commandment #1 Commandment #2	CIP-001-1a - R1 - R2 CIP-003-3 - R1 - R1.1 - R4 CIP-006-3c R1
Information Security - Management Support / Involvement	IS-02	Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution	経営陣と部門管理者は、文書による明確な方向づけ、自らの関与、暫約、明確な任務、任務の実行の検証を通して、情報セキュリティを正式に支持すること。								X	X	X	X	X		DS5.1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	Clause 5 A.6.1.1	CM-1 PM-1 PM-11	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	12.5	C.1		8.2.1	Commandment #3 Commandment #6	CIP-003-3 - R1 - R1.1
Information Security - Policy	IS-03	Management shall approve a formal information security policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy shall be supported by a strategic plan and a security program with well defined roles and responsibilities for leadership and officer roles.	情報セキュリティ基本方針文書は、経営陣によって正式に承認され、従業員や契約相手、関連する外部関係者に公表し、通知すること。情報セキュリティ基本方針は、組織の方向性を確立し、ベストプラクティスや適用可能な規制、国内法、国際法に整合していること。また、経営陣の役割や責任が明確に定義された戦略計画やセキュリティ計画によって支援(support)すること。								X	X	X	X	X	X	DS5.2	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i) 45 CFR 164.316 (b)(2)(ii) 45 CFR 164.308(a)(2)	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2	AC-1 AT-1 AU-1 CA-1 CM-1 IA-1 IR-1 MA-1 MP-1 MP-1 PE-1 PL-1 PS-1 SA-1 SC-1 SI-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SI-1	12.1 12.2	B.1		8.1.0 8.1.1	Commandment #1 Commandment #2 Commandment #3	CIP-003-3 - R1 -R1.1 - R1.2 - R2 - R2.1 - R2.2 - R2.3
Information Security - Baseline Requirements	IS-04	Baseline security requirements shall be established and applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements. Compliance with security baseline requirements must be reassessed at least annually or upon significant changes.	基準となるセキュリティ要求事項を確立し、(開発または購入する)アプリケーションやデータベース、システム、ネットワークインフラ、情報処理の設計、実装が施策や標準、規制との要求事項を満たすようにすること。基準となるセキュリティ要求事項の遵守状況は、少なくとも年に一回、もしくは重大な変化が生じた際に見直さなければならない。	セキュリティ要求事項には、アクセス管理、脆弱性対策、監査用ログの取得、物理的安全管理措置、などが含まれている事。	X	X	X	X	X	X	X	X	X	X	X		AI2.1 AI2.2 AI3.3 DS2.3 DS11.6		A.12.1.1 A.15.2.2	CM-2 SA-2 SA-4	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 SA-2 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)	1.1 1.1.1 1.1.2 1.1.3 1.1.4 1.1.5 1.1.6 2.2 2.2.1 2.2.2 2.2.3 2.2.4	L.2, L.5, L.7 L.8, L.9, L.10	L.2	1.2.6 8.2.1 8.2.7	Commandment #2 Commandment #4 Commandment #5 Commandment #11	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Information Security - Policy Reviews	IS-05	Management shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.	情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変更が発生した場合に、それが引き続き適切、妥当、及び有効であることを確実にするために、経営陣がレビューすること。	Proposed v1.1 control revision redacted due to potential mapping impact not yet considered: Security policy changes with material operational impact must require formal notification of subcontractors, tenants, supporting service tiers and employees of the impact and ramifications. 運用の変更を伴うセキュリティ方針の変更は、その影響および派生を考慮し、請負、テナント、およびそれに関わるサービス業者および雇用者に正式に通知される事。							X	X	X	X	X	X	DS 5.2 DS 5.4	45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306€	Clause 4.2.3 f) A.5.1.2	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-5 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 SA-1 SC-1 SI-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CP-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-5 (1) NIST SP800-53 R3 IA-5 (2) NIST SP800-53 R3 IA-5 (3) NIST SP800-53 R3 IA-5 (6) NIST SP800-53 R3 IA-5 (7) NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 RA-1 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SI-1	12.1.3	B.1.33. B.1.34,	B.2	1.2.1 8.2.7 10.2.3	Commandment #1 Commandment #2 Commandment #3	CIP-003-3 - R1.2 - R3.3 - R1.3 R3 - R3.1 - R3.2 - R3.3
Information Security - Policy Enforcement	IS-06	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures.	セキュリティ方針や手順に違反した従業員に対する正式な懲戒あるいは制裁ポリシーを備えること。違反した場合にどのような措置が講ぜられるのかについて方針や手順に明記され、従業員はそれを認識すること。	通販や健康情報等機微情報を取扱うシステムでは、誓約書提出なども併せて行う事							X	X	X	X	X	X	PO 7.7	45 CFR 164.308 (a)(1)(ii)(C)	A.8.2.3	PL-4 PS-1 PS-8	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-8		B.1.5		10.2.4	Commandment #6 Commandment #7	
Information Security - User Access Policy	IS-07	User access policies and procedures shall be documented, approved and implemented for granting and revoking normal and privileged access to applications, databases, and server and network infrastructure in accordance with business, security, compliance and service level agreement (SLA) requirements.	利用者アクセス制御ポリシーや手順は、業務上、セキュリティ上、法令上、及びSLAの要求事項に基づいて文書化し、承認し、導入すること。制御方針では、アプリケーションやデータベース、サーバ、ネットワークインフラへのアクセス権（一般および特権）の許可及び取り消しについて定めること。		X	X	X	X	X	X	X	X	X	X	X		DS 5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312 (a)(1) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.308(a)(4)(ii)(B) 45 CFR 164.308(a)(4)(ii)(C)	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	AC-1 IA-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 IA-1	3.5.1 8.5.1 12.5.4	B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	B.1	8.1.0	Commandment #6 Commandment #7 Commandment #8	CIP-007-3 - R5.1 - R5.1.2
Information Security - User Access Restriction / Authorization	IS-08	Normal and privileged user access to applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted.	アプリケーションやシステム、データベース、ネットワーク構成、機密データや機能への一般及び特権利用者のアクセスは、事前に管理者により承認され、制限されること。			X	X	X	X	X		X	X	X	X	X	DSS.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	A.11.2.1 A.11.2.2 A.11.4.1 A.11.4.2 A.11.6.1	AC-3 AC-5 AC-6 IA-2 IA-4 IA-5 IA-8 MA-5 PS-6 SA-7 SI-9	NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-3 (3) NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-2 (1) NIST SP800-53 R3 IA-2 (2) NIST SP800-53 R3 IA-2 (3) NIST SP800-53 R3 IA-2 (8) NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-4 (4) NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-5 (1) NIST SP800-53 R3 IA-5 (2) NIST SP800-53 R3 IA-5 (3) NIST SP800-53 R3 IA-5 (6) NIST SP800-53 R3 IA-5 (7) NIST SP800-53 R3 IA-8 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-9	7.1 7.1.1 7.1.2 7.1.3 7.2.1 7.2.2 8.5.1 12.5.4	H.2.4, H.2.5,		8.2.2	Commandment #6 Commandment #7 Commandment #8 Commandment #9 Commandment #10	CIP-003-3 - R5.1.1 - R5.3 CIP-004-3 R2.3 CIP-007-3 R5.1 - R5.1.2
Information Security - User Access Revocation	IS-09	Timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data shall be implemented upon any change in status of employees, contractors, customers, business partners or third parties. Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.	組織のシステムや情報資産、データへのアクセス権は、従業員、契約相手、顧客、事業パートナー、もしくは第三者の雇用もしくは契約や合意の終了時、または組織内の異動や雇用の変更時に遅滞停止、削除、変更すること。	通販や健康情報等機微情報を取扱うシステムでは半月以内に実施されている事	X	X	X	X	X	X		X	X	X	X		DS 5.4	45 CFR 164.308(a)(3)(ii)(C)	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	AC-2 PS-4 PS-5	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5	8.5.4 8.5.5	E.6.2, E.6.3	H.2	8.2.1	Commandment #6 Commandment #7 Commandment #8	CIP-004-3 R2.2.3 CIP-007-3 - R5.1.3 -R5.2.1 - R5.2.3
Information Security - User Access Reviews	IS-10	All levels of user access shall be reviewed by management at planned intervals and documented. For access violations identified, remediation must follow documented access control policies and procedures.	管理者は、利用者のアクセス権をあらかじめ定められた間隔でレビューし、記録を残すこと。アクセス権の違反を発見した場合は、文書化されたアクセス制御方針・手順に従い、是正処置を施すこと。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Periodic attestation of entitlement rights for all system users is required. Attestation for entitlement rights should extend to users in supporting service tiers (IaaS, SaaS, PaaS, IDaaS…). Automatic or manual remediation shall be implemented for identified violations.全システムユーザの権限(資格)は、定期的に証明(検査)されること。権限(資格) の証明は、間接的な支援サービス層(IaaS, SaaS, PaaS, IDaaS…)まで行うこと。違反が判明した場合には、自動または手動による対策を導入する事。	X	X	X	X	X	X		X	X	X	X	X	DSS.3 DSS.4	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	A.11.2.4	AC-2 AU-6 PM-10 PS-6 PS-7	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7		H.2.6, H.2.7, H.2.9,		8.2.1 8.2.7	Commandment #6 Commandment #7 Commandment #8 Commandment #10	CIP-004-3 R2.2.2 CIP-007-3 - R5 - R.1.3
Information Security - Training / Awareness	IS-11	A security awareness training program shall be established for all contractors, third party users and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, process and policies, relating to their function relative to the organization.	組織のすべての従業員、及び契約相手、第三者の利用者に対し、セキュリティ意識向上の教育プログラムを構築し、妥当であれば強制的に実施すること。組織のデータにアクセスする、すべての者が、職務に関連する組織の方針・手順・手続きについての適切な意識向上のための教育・訓練を受け、また定期的な更新を受けること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: A security awareness training program that addresses multi-tenant, nationality and cloud delivery model SOD and conflicts of interest shall be established for all contractors, third party users, tenants and employees of the organization. All individuals with access to tenant data shall receive appropriate awareness training and regular updates in organizational procedures, process and policies, relating to their function relative to the organization. セキュリティ意識向上のための教育プログラムでは、マルチテナント、国民性、クラウドデリバリモデル SOD、利害不一致などを網羅している事、対象は、契約社員(従業員)、サード/パーティのユーザ、テナント、および組織の社員の全て行うこと。テナントのデータにアクセスがある全員が、適切な教育を受け、社内の役割に応じて、社内手順、プロセス、方針について定期的に更新・変更を確認する事。	X	X	X	X	X	X	X	X	X	X	X	X	PO 7.4	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	Clause 5.2.2 A.8.2.2	AT-1 AT-2 AT-3 AT-4	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	12.6 12.6.1 12.6.2	E.4	E.1	1.2.10 8.2.1	Commandment #3 Commandment #6	CIP-004-3 - R1 - R2 - R2.1
Information Security - Industry Knowledge / Benchmarking	IS-12	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.	セキュリティに関する研究会や会議、セキュリティの専門家による協会や団体との適切な連絡体制を維持すること。								X	X	X	X	X	X			A.6.1.7	AT-5 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 SI-5		C.1.8			Commandment #1 Commandment #2 Commandment #3	
Information Security - Roles / Responsibilities	IS-13	Roles and responsibilities of contractors, employees and third party users shall be documented as they relate to information assets and security.	情報資産やセキュリティへの関わりに応じて、従業員、契約相手及び第三者の利用者の役割や責任を文書に定めること。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.1		Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1	AT-3 PL-4 PM-10 PS-1 PS-6 PS-7	NIST SP800-53 R3 AT-3 NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7		B.1.5, D.1.1,D.1.3.3, E.1, F.1.1, H.1.1, K.1.2	B.1	1.2.9 8.2.1	Commandment #6 Commandment #7 Commandment #8	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Information Security - Management Oversight	IS-14	Managers are responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility.	管理者は、自らの責任範囲に関わるセキュリティ方針、手順、標準について認識し、順守する責任がある								X	X	X	X	X	X	DS5.3 DS5.4 DS5.5		Clause 5.2.2 A.8.2.1 A.8.2.2 A.11.2.4 A.15.2.1	AT-2 AT-3 CA-1 CA-5 CA-6 CA-7 PM-10	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PM-10	12.6.1 12.6.2	E.4	E.1	1.1.2 8.2.1	Commandment #6 Commandment #7 Commandment #8	
Information Security - Segregation of Duties	IS-15	Policies, process and procedures shall be implemented to enforce and assure proper segregation of duties. In those events where user-role conflict of interest constraint exist, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.	適切な職務の分割を確実に実施するための方針、手続き、手順を確立すること。利用者役割に利害の対立が存在する場合、組織の情報資産の許可されていないまたは意図しない変更または誤用の危険性を低減するための技術的管理策を導入すること。		X	X	X	X	X	X	X	X	X	X	X		DS 5.4	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(i)(A) 45 CFR 164.308(a)(4)(i)(A) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.3	AC-1 AC-2 AC-5 AC-6 AU-1 AU-6 SI-1 SI-4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6)	6.4.2	G.2.13. G.3, G.20.1, G.20.2, G.20.5		8.2.2	Commandment #6 Commandment #7 Commandment #8 Commandment #10	CIP-007-3 R5.1.1
Information Security - User Responsibility	IS-16	Users shall be made aware of their responsibilities for: ・Maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements ・Maintaining a safe and secure working environment ・Leaving unattended equipment in a secure manner	利用者は以下の責任を認識すること。 ・公表されたセキュリティ方針、手順、標準、関連する規制上の要求事項を認識し、順守すること ・安全、安心な職場環境を維持すること ・無人状態にある装置の保護措置を講ずること		X	X	X	X	X	X	X	X	X	X	X	X	PO 4.6	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	AT-2 AT-3 AT-4 PL-4	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4 NIST SP800-53 R3 PL-4	8.5.7 12.6.1	E.4	E.1	1.2.10 8.2.1	Commandment #5 Commandment #6 Commandment #7	
Information Security - Workspace	IS-17	Policies and procedures shall be established for clearing visible documents containing sensitive data when a workspace is unattended and enforcement of workstation session logout for a period of inactivity.	無人の作業場所において、機密データを含む文書が閲覧されることがないように、また不使用時にはワークステーションのセッションを強制ログアウトするように、方針、手順を確立すること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Policies and procedures shall be established for proper data management within the provider environment. Policies and procedures must resolve conflicts of interests and include a tamper audit function, that trips a tamper audit to the customer if the integrity of the tenant data has potentially been compromised. (access not authorized by tenant or data loss) プロバイダの環境において、適切なデータ管理用に方針や手順が定められている事。方針や手順は、改ざん監査機能などの利害の不一致などを想定し解決策を有する事。テナントのデータの完全性が侵害されているか、ユーザに対する監査/テナントが許可していないデータまたはデータ損失)なども考慮する事。	X					X	X	X	X	X	X	X			Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3	AC-11 MP-2 MP-3 MP-4	NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-2 (1) NIST SP800-53 R3 MP-3 NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-4 (1)		E.4	E.1	8.2.3	Commandment #5 Commandment #6 Commandment #7 Commandment #11	
Information Security - Encryption	IS-18	Policies and procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).	ストレージ（例えば、ファイルサーバ、データベース、エンドユーザ側のワークステーション）内の機密データや伝送中のデータ（例えば、システムインタフェース、公衆ネットワーク上、電子メールなど）を暗号化するための方針、手順を確立すること	暗号化の強度は、最低でも脆弱性が発見されていない物を採用する事。		X	X	X	X	X	X	X	X	X	X		DS5.8 DS5.10 DS5.11	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 A.12.3.1 A.15.1.3 A.15.1.4	AC-18 IA-3 IA-7 SC-7 SC-8 SC-9 SC-13 SC-16 SC-23 SI-8	NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST SP800-53 R3 AC-18 (5) NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18) NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-8 (1) NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1) NIST SP800-53 R3 SC-13	2.1.1 3.4 3.4.1 4.1 4.1.1 4.2	G.10.4, G.11.1, G.11.2, G.12.1, G.12.2, G.12.4, G.12.10, G.14.18, G.14.19, G.16.2, G.16.18, G.16.19, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	G.4 G.15 I.3	8.1.1 8.2.1 8.2.5	Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11	CIP-003-3 - R4.2
Information Security - Encryption Key Management	IS-19	Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.	ストレージ内や伝送中のデータの暗号化を支援するために、効果的な鍵管理のための方針、手順を確立し、実施すること。			X		X	X	X	X	X	X	X	X		DS5.8	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1)	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	SC-12 SC-13 SC-17 SC-28	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-12 (2) NIST SP800-53 R3 SC-12 (5) NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-28 NIST SP800-53 R3 SC-28 (1)	3.4.1 3.5 3.5.1 3.5.2 3.6 3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7 3.6.8	L.6		8.1.1 8.2.1 8.2.5	Commandment #9 Commandment #10 Commandment #11	
Information Security - Vulnerability / Patch Management	IS-20	Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.	脆弱性やパッチ管理の方針、手順を確立し、実施すること、それにより、アプリケーション やシステム、ネットワーク機器の脆弱性を確実に評価し、重要なパッチを優先的に適用するリスクベースの手法により、ベンダーが供給するセキュリティパッチを迅速に適用できるようにすること。			X	X	X	X		X	X	X	X	X		AI6.1 AI3.3 DS5.9	45 CFR 164.308 (a)(1)(ii)(A) 45 CFR 164.308 (a)(1)(ii)(B) 45 CFR 164.308 (a)(5)(ii)(B)	A.12.5.1 A.12.5.2 A.12.6.1	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5	NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 RA-5 NIST SP800-53 R3 RA-5 (1) NIST SP800-53 R3 RA-5 (2) NIST SP800-53 R3 RA-5 (3) NIST SP800-53 R3 RA-5 (9) NIST SP800-53 R3 RA-5 (6) NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-2 (2) NIST SP800-53 R3 SI-5	2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3	G.15.2, I.3	I.4	1.2.6 8.2.7	Commandment #4 Commandment #5	CIP-004-3 R4 - 4.1 - 4.2 CIP-005-3a - R1 - R1.1 CIP-007-3 - R3 - R3.1 - R8.4

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Information Security - Anti-Virus / Malicious Software	IS-21	Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.	アンチウイルスプログラムが、すべての既知のマルウェア、もしくは認可されていないソフトウェアを検知し、除去することができるように、アンチウイルス・シグネチャを少なくとも12時間おきにアップデートすること。			X	X	X	X			X	X	X	X	X	DS5.9	45 CFR 164.308 (a)(5)(ii)(B)	A.10.4.1	SA-7 SC-5 SI-3 SI-5 SI-7 SI-8	NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-5 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1) NIST SP800-53 R3 SI-8	5.1 5.1.1 5.2	G.7		8.2.2	Commandment #4 Commandment #5	CIP-007-3 - R4 - R4.1 - R4.2
Information Security - Incident Management	IS-22	Policies and procedures shall be established to triage security related events and ensure timely and thorough incident management.	セキュリティ関連事象を選別し、迅速で完全なインシデント管理を確実に行うための方針、手順を確立すること。	Control revision v1.1 rationale: Minor editorial correction.	X	X	X	X	X	X	X	X	X	X	X	X	DS5.6	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	Clause 4.3.3 A.13.1.1 A.13.2.1	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-3 NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-4 (1) NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 IR-8	12.9 12.9.1 12.9.2 12.9.3 12.9.4 12.9.5 12.9.6	J.1.1, J.1.2	J.1	1.2.4 1.2.7 7.1.2 7.2.2 7.2.4 10.2.1 10.2.4	Commandment #2 Commandment #6 Commandment #8	CIP-007-3 - R6.1 CIP-008-3 - R1
Information Security - Incident Reporting	IS-23	Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements.	従業員、契約相手、第三者利用者は、あらゆる情報セキュリティ事象を迅速に報告する責任があることを認識すること。情報セキュリティ事象は、法律、規制、契約上の要求事項に従って、あらかじめ決められた連絡経路を通じて迅速かつ適切に報告すること。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.6	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) 16 CFR 318.5 (a) 45 CFR 160.410 (a)(1)	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	IR-2 IR-6 IR-7 SI-4 SI-5	NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-6 (1) NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6) NIST SP800-53 R3 SI-5	12.5.2 12.5.3	J.1.1, E.4	J.1 E.1	1.2.7 1.2.10 7.1.2 7.2.2 7.2.4 10.2.4	Commandment #2 Commandment #6 Commandment #8	CIP-003-3 - R4.1 CIP-004-3 R3.3
Information Security - Incident Response Legal Preparation	IS-24	In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.	情報セキュリティインシデント発生後に、個人もしくは組織に関わる事後措置として法的措置が必要になる場合に備え、証拠の収集、保存、提出を行うための、追跡調査ができる適切なフォレンジック手順を確立すること。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.6	45 CFR 164.308 (a)(6)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3	AU-6 AU-7 AU-9 AU-11 IR-5 IR-7 IR-8	NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-7 (1) NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 IR-8		J.1.1, J.1.2, E.4	J.1 E.1	1.2.7		CIP-004-3 R3.3
Information Security - Incident Response Metrics	IS-25	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	情報セキュリティインシデントのタイプ、件数、コストを測定・定量化するための仕組みを導入すること。		X	X	X	X	X	X	X	X	X	X	X	X	DS 4.9	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2	IR-4 IR-5 IR-8	NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-4 (1) NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-8	12.9.6	J.1.2		1.2.7 1.2.10		CIP-008-3 - R1.1
Information Security - Acceptable Use	IS-26	Policies and procedures shall be established for the acceptable use of information assets.	情報資産の利用の許容範囲に関する方針、手順を確立すること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Policies and procedures shall be established for the acceptable use of information assets. The policies shall address acceptable data mining functionality and Traffic pattern analysis. And shall inform the tenant who is getting access to the data analysis output. 情報資産の利用について、適切な方針および手順を定める事。方針では、適切なデータマイニングおよびトラフィックパターン分析についても網羅する事。また、そのデータ分析結果にアクセス可能なテナントに対して適宜告知すること。					X	X	X	X	X	X	X	X	DS 5.3	45 CFR 164.310 (b)	A.7.1.3	AC-8 AC-20 PL-4	NIST SP800-53 R3 AC-8 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 AC-20 (1) NIST SP800-53 R3 AC-20 (2) NIST SP800-53 R3 PL-4	12.3.5	B.1.7, D.1.3.3, E.3.2, E.3.5.1, E.3.5.2	B.3	8.1.0	Commandment #1 Commandment #2 Commandment #3	
Information Security - Asset Returns	IS-27	Employees, contractors and third party users must return all assets owned by the organization within a defined and documented time frame once the employment, contract or agreement has been terminated.	従業員、契約相手及び第三者の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産すべてを、文書で定められた所定の期間内に返却しなければならない。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Controls shall be put in place to insure privacy and automate tenant breach formal notification upon the compromise of a tenant's system(s). テナントのシステムが侵害された場合、プライバシーの保護を緩和し、自動的にテナントの侵害を正式に通知する制御(規制)を導入する事。	X	X	X	X	X	X	X	X	X	X	X	X		45 CFR 164.308 (a)(3)(ii)(C)	A.7.1.1 A.7.1.2 A.8.3.2	PS-4	NIST SP800-53 R3 PS-4		E.6.4	D.1	5.2.3 7.2.2 8.2.1 8.2.6		
Information Security - eCommerce Transactions	IS-28	Electronic commerce (e-commerce) related data traversing public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure or modification in such a manner to prevent contract dispute and compromise of data.	公衆ネットワークを経由してデータをやり取りする電子商取引は、不正行為、許可されていない開示や改ざんのような行為から契約上の紛争やデータの漏洩を防ぐために、適切に分類され保護されなければならない。			X				X		X	X	X	X	X	DS 5.10 5.11	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	AC-14 AC-21 AC-22 IA-8 AU-10 SC-4 SC-8 SC-9	NIST SP800-53 R3 AC-14 NIST SP800-53 R3 AC-14 (1) NIST SP800-53 R3 AC-21 NIST SP800-53 R3 AC-22 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 AU-10 NIST SP800-53 R3 AU-10 (5) NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-8 (1) NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1)	2.1.1 4.1 4.1.1 4.2	G.19.1.1, G.19.1.2, G.19.1.3, G.10.8, G.9.11, G.14, G.15.1	G.4 G.11 G.16 G.18 I.3 I.4	3.2.4 4.2.3 7.1.2 7.2.1 7.2.2 8.2.1 8.2.5	Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11	
Information Security - Audit Tools Access	IS-29	Access to, and use of, audit tools that interact with the organizations information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	ログデータの悪用又は誤用を防ぐために、組織の情報システムの監査ツールへのアクセスや利用は制限されること。		X	X	X	X	X	X		X	X	X	X		DS 5.7		A.15.3.2	AU-9 AU-11 AU-14	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	10.5.5			8.2.1	Commandment #2 Commandment #5 Commandment #11	CIP-003-3 - R5.2
Information Security - Diagnostic / Configuration Ports Access	IS-30	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	診断用及び環境設定用ポートへのアクセスは、許可された個人またはアプリケーションに制限すること。		X				X			X	X	X	X	X	DS5.7		A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	CM-7 MA-3 MA-4 MA-5	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-3 (1) NIST SP800-53 R3 MA-3 (2) NIST SP800-53 R3 MA-3 (3) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5	9.1.2	H1.1, H1.2, G.9.15			Commandment #3 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8	CIP-007-3 - R2
Information Security - Network / Infrastructure Services	IS-31	Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.	ネットワークやインフラのサービスレベルアグリーメントには、組織が自ら提供するか外部委託しているかに関わらず、セキュリティコントロール制限、容量やサービスレベル、事業もしくは顧客の要求事項を明確に盛り込むこと。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.10		A.6.2.3 A.10.6.2	SC-20 SC-21 SC-22 SC-23 SC-24	NIST SP800-53 R3 SC-20 NIST SP800-53 R3 SC-20 (1) NIST SP800-53 R3 SC-21 NIST SP800-53 R3 SC-22 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SC-24		C.2.6, G.9.9	C.2	8.2.2 8.2.5	Commandment #6 Commandment #7 Commandment #8	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	ラップトップや携帯電話、PDAなどの可搬型機器は概して非可搬型機器(組織の施設内のデスクトップなど)に比べリスクが高いので、可搬型機器からの機密情報へのアクセスを厳格に制限する方針、手順を確立し、実施すること。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.11 DS5.5	45 CFR 164.310 (d)(1)	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	AC-17 AC-18 AC-19 MP-2 MP-4 MP-6	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-17 (1) NIST SP800-53 R3 AC-17 (2) NIST SP800-53 R3 AC-17 (3) NIST SP800-53 R3 AC-17 (4) NIST SP800-53 R3 AC-17 (5) NIST SP800-53 R3 AC-17 (7) NIST SP800-53 R3 AC-17 (8) NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST SP800-53 R3 AC-18 (5) NIST SP800-53 R3 AC-19 NIST SP800-53 R3 AC-19 (1) NIST SP800-53 R3 AC-19 (2) NIST SP800-53 R3 AC-19	9.7 9.7.2 9.8 9.9 11.1 12.3	G.11, G12, G.20.13, G.20.14		1.2.6 3.2.4 8.2.6	All	CIP-007-3 - R7.1
Information Security - Source Code Access Restriction	IS-33	Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis. Records shall be maintained regarding the individual granted access, reason for access and version of source code exposed.	アプリケーション、プログラムまたはオブジェクトソースコードへのアクセスは、許可された者に限定すること、アクセスした者やアクセスの理由、開示されたソースコードのバージョンについて記録を残すこと。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Access to application, program or object source code shall be restricted to authorized personnel based on cloud delivery model (PaaS) on a need to know basis. アプリケーション、プログラムまたはオブジェクトソースコードへのアクセスは、PaaS(クライドデリバリモデル)に基づき、知る必要に応じて権限を付与された担当者に限定される事。			X	X	X	X		X	X	X	X			Clause 4.3.3 A.12.4.3 A.15.1.3	CM-5 CM-6	NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3)	6.4.1 6.4.2	I.2.7.2, I.2.9, I.2.10, I.2.15		1.2.6 6.2.1	Commandment #6 Commandment #7 Commandment #9 Commandment #10	
Information Security - Utility Programs Access	IS-34	Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	システム及びオブジェクト、ネットワーク、仮想マシン、アプリケーション制御を無効にすることのできるユーティリティプログラムの使用は、制限すること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Utility programs and privileged management accounts capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted. Utilities that utilities that can shut down virtualized partitions shall be disallowed. Attacks that target the virtual infrastructure (Shimming, Blue Pill, Hyperjacking, etc.) shall be identified and remediated with technical and procedural controls. システム、オブジェクト、ネットワーク、仮想マシン、およびアプリケーション制御(設定)が再定義(オーバーライド)される可能性を考慮し、運用(ユーティリティ)ツールと特権管理用のアカウントの権限は制限される事。仮想パーティションのシャットダウンが可能なツールの利用を許可しない事。仮想基盤に対する攻撃手法 (Shimming、Blue Pill、Hyperjackingなど)を認識し、技術的および運用的な対策を適用する事。			X	X	X	X		X	X	X	X	X	X	DS5.7		A.11.4.1 A.11.4.4 A.11.5.4	AC-5 AC-6 CM-7 SC-3 SC-19	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-19	7.1.2	H.2.16			Commandment #1 Commandment #5 Commandment #6 Commandment #7	CIP-007-3 - R2.1 - R2.2 - R2.3
Legal - Non-Disclosure Agreements	LG-01	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented and reviewed at planned intervals.	データ保護や作業手順に対する組織のニーズを反映する守秘義務契約もしくは秘密保持契約のための要求事項は、特定し、文書化し、あらかじめ定められた間隔でレビューすること。							X	X	X	X	X	X	X			ISO/IEC 27001:2005 Annex A.6.1.5	PL-4 PS-6 SA-9	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)	12.8.2 12.8.3 12.8.4	C.2.5		1.2.5	Commandment #6 Commandment #7 Commandment #8 Commandment #9	
Legal - Third Party Agreements	LG-02	Third party agreements that directly, or indirectly, impact the organizations information assets or data are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assets agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	組織の情報資産またはデータに直接的もしくは間接的に影響を及ぼす第三者との契約は、関連するすべてのセキュリティ要求事項を明示的に取り上げること。これには、組織の情報資産の処理、アクセス、通信、ホスティングもしくは管理、又は既存の情報へのサービス又は製品の追加あるいは停止に関わる契約が含まれる。資産に関わる契約には、やり取りされるデータの不適切な開示や改変、破壊を防止するために、セキュリティ(例えば、暗号化、アクセス制御、消えい防止)や完全性の管理に関する条項を含むこと。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.11	45 CFR 164.308 (a)(4)(ii)(A) 45 CFR 164.308 (b)(1) 45 CFR 164.308 (b)(2)(i) 45 CFR 164.308 (b)(2)(ii) 45 CFR 164.308 (b)(2)(iii) 45 CFR 164.308 (b)(3) 45 CFR 164.308 (b)(4) 45 CFR 164.312(e)(2)(ii) 45 CFR 164.312 (c)(1) 45 CFR 164.312(e)(2)(ii) 45 CFR 164.314 (a)(1)(i) 45 CFR 164.314 (a)(1)(ii)(A) 45 CFR 164.314 (a)(2)(i) 45 CFR 164.314 (a)(2)(i)(A) 45 CFR 164.314 (a)(2)(i)(B) 45 CFR 164.314 (a)(2)(i)(C) 45 CFR 164.314 (a)(2)(i)(D) 45 CFR 164.314 (a)(2)(ii)(A) 45 CFR 164.314 (a)(2)(ii)(A)(1) 45 CFR 164.314 (a)(2)(ii)(A)(2) 45 CFR 164.314 (a)(2)(ii)(B) 45 CFR 164.314 (a)(2)(ii)(C) 45 CFR 164.314 (b)(1) 45 CFR 164.314 (b)(2) 45 CFR 164.314 (b)(2)(i) 45 CFR 164.314 (b)(2)(ii) 45 CFR 164.314 (b)(2)(iii) 45 CFR 164.314 (b)(2)(iv)	A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.,11.6.1 A.12.3.1 A.,12.5.4	CA-3 MP-5 PS-7 SA-6 SA-7 SA-9	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MP-5 NIST SP800-53 R3 MP-5 (2) NIST SP800-53 R3 MP-5 (4) NIST SP800-53 R3 PS-7 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)	2.4 12.8.2	C.2.4, C.2.6, G.4.1, G.16.3	C.2	1.2.5	Commandment #1 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8	
Operations Management - Policy	OP-01	Policies and procedures shall be established and made available for all personnel to adequately support services operations role.	サービスあるいは運用の役割を十分支援するために、方針や手順は、すべての従業員に対して作成され利用可能とすること。					X	X	X	X	X	X	X	X		DS13.1		Clause 5.1 A 8.1.1 A.8.2.1 A.8.2.2 A.10.1.1	CM-2 CM-3 CM-4 CM-5 CM-6 CM-9 MA-4 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-12	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3) NIST SP800-53 R3 CM-9 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 SA-12	12.1 12.2 12.3 12.4	G.1.1		8.2.1	Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Operations Management - Documentation	OP-02	Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure the following: ・Configuring, installing, and operating the information system ・Effectively using the system's security features	情報システム文書（例えば、管理者及び利用者ガイド、構成図など）は、以下を確実に行うために、認可された従業員に対して利用可能とすること。 ・情報システムの設定、インストール、操作 ・システムのセキュリティ機能の効果的な利用			X	X	X	X	X	X	X	X	X	X		DS 9 DS 13.1		Clause 4.3.3 A.10.7.4	CP-9 CP-10 SA-5 SA-10 SA-11	NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1)	12.1 12.2 12.3 12.4	G.1.1		1.2.6	Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11	CIP-005-3a - R1.3 CIP-007-3 - R9
Operations Management - Capacity / Resource Planning	OP-03	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	規制、契約、事業上の要求事項に基づき、要求されたシステム性能を実現するために、可用性、品質、十分な容量や資源について計画、準備、測定を行うこと。また、システムの過負荷のリスクを低減するために、将来必要とする容量を予測すること。			X	X	X		X		X	X	X	X	X	DS 3		A.10.3.1	SA-4	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)		G.5		1.2.4	Commandment #1 Commandment #2 Commandment #3	
Operations Management - Equipment Maintenance	OP-04	Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.	運用の継続性及び可用性を保証するための機器のメンテナンスのために、方針及び手順を確立すること。		X	X	X	X	X	X	X	X	X	X	X		A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	MA-2 MA-3 MA-4 MA-5 MA-6	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-2 (1) NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-3 (1) NIST SP800-53 R3 MA-3 (2) NIST SP800-53 R3 MA-3 (3) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5 NIST SP800-53 R3 MA-6		F.2.19		5.2.3 8.2.2 8.2.3 8.2.4 8.2.5 8.2.6 8.2.7	Commandment #2 Commandment #5 Commandment #11	CIP-007-3 - R6.1 - R6.2 - R6.3 - R6.4
Risk Management - Program	RI-01	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	組織は、リスクを受容可能なレベルに抑えるための、事業リスク管理の枠組みを作成し、維持すること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Organizations shall develop and maintain a cloud oriented risk management framework to manage risk as defined in the master agreement or industry best-practices and standards. 主契約内で定められるまたは業界ベストプラクティスおよびスタンダードに従い、クラウド志向のリスク管理フレームワークを作成し維持し、リスク管理する事。	X	X	X	X	X	X	X	X	X	X	X	X	PO 9.1	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.6.1 A.14.1.2 A.15.2.1 A.15.2.2	AC-4 CA-2 CA-6 PM-9 RA-1	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-6 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 RA-1	12.1.2	A.1, L.1	L.2	1.2.4		CIP-009-3 - R4
Risk Management - Assessments	RI-02	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	事業全体の枠組みと連携し、公式のリスクアセスメントを少なくとも年に1回又はあらかじめ定められた間隔で実施し、特定したすべてのリスクの蓋然性や影響度を定性的、定量的手法を用いて測定すること。固有リスク及び残余リスクの蓋然性や影響度は、すべてのリスク分類（例えば、監査結果、脅威・脆弱性分析、法規制の順守など）を考慮し、独立して測定すること。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Service Providers shall implement and communicate disaster recovery, business continuity, capacity overflow and operational redundancy plans to all dependant service tiers. Service Providers shall perform failure impact analysis studies and communicate potential service impacts and reduced capacity projections to tenants. Tenants shall be afforded access to operational redundancy and continuity summaries which shall include dependant service tier oriented impact analysis. Security mechanisms and redundancies (at a minimum of N+2 at all times) shall be implemented to protect physical and virtual machines, networks, service providers and hardware from service outages (e.g., power failures, network disruptions, etc.). Tenants shall access to a tenant triggered failover control. サービスプロバイダは全サービス層において、災害復旧、事業継続、許容超過、運用冗長化計画を導入し共有する事。サービスプロバイダは、障害による影響度分析を実施し、サービスへの影響および有事時の低めの容量をテナントと共有する事。テナントは、サービス別の影響度分析を含む運用冗長および事業継続概要の開覧が可能である事。停電、ネットワーク障害などに備え、セキュリティの仕組みおよび冗長化(常時、数量+2を必須とする)を導入し、物理および仮想マシン、ネットワーク、サービスプロバイダ、およびハードウェアを導入する事。テナントは、テナント自身が発動可能なフェールオーバーにアクセスできる事。	X	X	X	X	X	X	X	X	X	X	X	X	PO 9.4	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2	PL-5 RA-2 RA-3	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	12.1.2	C.2.1, I.4.1, I.5, G.15.1.3, I.3	I.1 I.4	1.2.4 1.2.5		CIP-002-3 - R1.1 - R1.2 CIP-005-3a - R1 - R1.2 CIP-009-3 - R.1.1
Risk Management - Mitigation / Acceptance	RI-03	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.	リスクは、受容可能なレベルに低減すること。リスク基準に基づく受容レベルは、妥当な決議の時間枠や経営陣の承認に従って確立し、文書化すること。		X	X	X	X	X	X	X	X	X	X	X	X	PO 9.5	45 CFR 164.308 (a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 4.3.1 Clause 5.1 f) Clause 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2	CA-5 CM-4	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4		I.3, L.9, L.10	I.4 L.2			CIP-009-3 - R1.2
Risk Management - Business / Policy Change Impacts	RI-04	Risk assessment results shall include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective.	リスクアセスメントの結果が適切かつ有効であり続けるように、リスクアセスメントの結果をセキュリティ基本方針、手順、標準、管理策に反映すること。		X	X	X	X	X	X	X	X	X	X	X	X	PO 9.6		Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2	CP-2 RA-2 RA-3	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	12.1.3	B.1.1, B.1.2, B.1.6, B.1.7.2, G.2, L.9, L.10	B.2 G.21 L.2			CIP-009-3 - R2
Risk Management - Third Party Access	RI-05	The identification, assessment, and prioritization of risks posed by business processes requiring third party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	組織の情報システムやデータへの第三者のアクセスを要するビジネスプロセスによるリスクの特定、評価、優先順位づけを行った後に、許可されていない又は不適切なアクセスの蓋然性や影響度を測定、監視、最小化するための資源の配分調整を行うこと。アクセスを提供する前に、リスク分析から導き出された補填的管理策を実施すること。		X	X	X	X	X	X	X	X	X	X	X	X	DS 2.3		A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4	CA-3 MA-4 RA-3	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 RA-3	12.8.1 12.8.2 12.8.3 12.8.4	B.1.1, B.1.2, D.1.1, E.1, F.1.1, H.1.1, K.1.1, E.6.2, E.6.3	B.1 H.2	7.1.1 7.1.2 7.2.1 7.2.2 7.2.3 7.2.4		

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability								
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Release Management - New Development / Acquisition	RM-01	Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.	新しいアプリケーション、システム、データベース、インフラ、サービス、運用、設備の開発又は購入についての経営陣の承認に関する方針や手順を確立すること。		X	X	X	X	X	X	X	X	X	X	X		A12 A16.1		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4	CA-1 CM-1 CM-9 PL-1 PL-2 SA-1 SA-3 SA-4	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 PL-2 (2) NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)	6.3.2	I.1.1, I.1.2, I.2. 7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5	I.2	1.2.6	Commandment #1 Commandment #2 Commandment #3	
Release Management - Production Changes	RM-02	Changes to the production environment shall be documented, tested and approved prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.	本番環境の変更は、実施前に文書化し、検証し、承認されなければならない。本番ソフトやハードの変更には、パッチやサービスパック、その他の更新や修正を必要とするアプリケーション、システム、データベース、ネットワーク機器が含まれる。			X	X	X	X	X	X	X	X	X	X	X	A16.1 A17.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2	CA-1 CA-6 CA-7 CM-2 CM-3 CM-5 CM-6 CM-9 PL-2 PL-5 SI-2 SI-6 SI-7	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3) NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 PL-2 (2) NIST SP800-53 R3 PL-5 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-2 (2) NIST SP800-53 R3 SI-6 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1)	1.1.1 6.3.2 6.4 6.1	I.2.17, I.2.20, I.2.22		1.2.6	Commandment #1 Commandment #2 Commandment #3 Commandment #11	CIP-003-3 - R6
Release Management - Quality Testing	RM-03	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed by the organization. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release.	組織が開発しているすべてのソフトウェアが品質基準を満たしているかを確認するための体系的な監視や評価の仕組みを確立すること。情報システムやアップグレード、新バージョンの品質評価や受入れ基準を確立し、文書化すること。また、セキュリティを維持するために、システムのテストは、開発中及び受入れ前に実施すること。管理者は、品質テスト過程において明確な監視能力を持ち、最終成果物が「目的に合致している」(成果物が意図した目的に適している)こと、そして「リリース前に「適正であること」(間違が除去されている)ことを証明できなければならない。			X	X	X	X	X	X	X	X	X			PO 8.1		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	CM-1 CM-2 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-13	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 SA-13	1.1.1 6.1 6.4	C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, I.22.1, I.22.3, I.22.6, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14,I.2.20, I.2.17, I.2.7.1, I.3, J.2.10, L.9		9.1.0 9.1.1 9.2.1 9.2.2	Commandment #1 Commandment #2 Commandment #3	
Release Management - Outsourced Development	RM-04	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all outsourced software development. The development of all outsourced software shall be supervised and monitored by the organization and must include security requirements, independent security review of the outsourced environment by a certified individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control shall be defined as either a ISO/IEC 17024 accredited certification or a legally recognized license or certification in the legislative jurisdiction the organization outsourcing the development has chosen as its domicile.	外部委託によって開発したソフトウェアが品質基準を満たしているかを確認するための体系的な監視や評価の仕組みを確立すること。外部委託によるすべてのソフトウェア開発の監督、監視を行い、セキュリティ要求事項の確認、資格ある者による外部委託先の開発環境の独立したセキュリティ・レビュー、外注先に対する公認のセキュリティ教育の実施、ソフトウェアコードのレビューなども実施すること。こうした管理の目的は、ISO/IEC 17024標準の認証又は法的に認められた認可、または開発を外部委託している組織の本籍地における認証によって担保されること。			X	X	X	X	X	X	X	X	X	X	X			A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.5 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	SA-4 SA-5 SA-8 SA-9 SA-10 SA-11 SA-12 SA-13	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1) NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SA-13	3.6.7 6.4.5.2 7.1.3 8.5.1 9.1 9.1.2 9.2b 9.3.1 10.5.2 11.5 12.3.1 12.3.3	C.2.4, G.4, G6, I.1, I.4.4, I.4.5, I.2.7.2, I.2.8, I.2.9, I.2.15, I.2.18, I.2.22.6, I.2.7.1, I.2.13, I.2.14, I.2.17, I.2.20, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14, I.3, J.1.2.10, L.7, L.9, L.10	C.2 I.1 I.2 I.4		Commandment #1 Commandment #2 Commandment #3	
Release Management - Unauthorized Software Installations	RM-05	Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.	認可されていないソフトウェアの導入を禁止するための方針や手順を確立し、実施すること。			X	X	X	X		X	X	X	X	X				A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 A.12.5.3	CM-1 CM-2 CM-3 CM-5 CM-7 CM-8 CM-9 SA-6 SA-7 SI-1 SI-3 SI-4 SI-7	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 CM-8 NIST SP800-53 R3 CM-8 (1) NIST SP800-53 R3 CM-8 (3) NIST SP800-53 R3 CM-8 (5) NIST SP800-53 R3 CM-9 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6) NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1)		G.2.13, G.20.2,G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23	G.1 I.2	3.2.4 8.2.2	Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11	
Resiliency - Management Program	RS-01	Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident.	認識されているリスク事象の影響を受容可能なレベルにまで最少化するために、事業継続性や災害復旧を規定する方針、プロセス、手順を確立し、法規制や契約、事業の要求事項に基づき、また業界標準に即した予防措置と復旧措置を組み合わせて、(たとえば、自然災害や事故、装置故障、意図的な行為の結果、影響を受けた)情報資産の回復を促進すること。この回復能力管理計画は、採用する前に知る必要のある組織の全従業員に伝達し、公表、保管、記録し、インシデント発生時にアクセスできなければならない複数の施設に配布すること。		X	X	X	X	X	X	X	X	X	X	X	X	PO 9.1 PO 9.2 DS 4.2	45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(C)	Clause 4.3.2 A.14.1.1 A.14.1.4	CP-1 CP-2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2)	12.9.1	K.1.2.9, K.1.2.10, K.3.1			Commandment #1 Commandment #2 Commandment #3	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Resiliency - Impact Analysis	RS-02	There shall be a defined and documented method for determining the impact of any disruption to the organization which must incorporate the following: ・Identify critical products and services ・Identify all dependencies, including processes, applications, business partners and third party service providers ・Understand threats to critical products and services ・Determine impacts resulting from planned or unplanned disruptions and how these vary over time ・Establish the maximum tolerable period for disruption ・Establish priorities for recovery ・Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption ・Estimate the resources required for resumption	あらゆるスや断の影響度を測定するための方法をあらかじめ規定し、文書化しておくこと。その方法には以下が含まれなければならない。 ・重要な製品やサービスの特定 ・プロセス、アプリケーション、ビジネスパートナー、第三者のサービスプロバイダを含むすべての依存関係の特定 ・重要な製品やサービスへの脅威の認識 ・計画した中断又は計画外の中断に起因する影響、及びそうした中断が時間と共にどのように変化するかの測定 ・中断を許容しうる最長期間の設定 ・復旧の優先順位の設定 ・最長中断許容時間内にある重要製品・サービスの再開に向けた復旧目標時間の設定 ・再開に向けた資源の見積もり		X	X	X	X	X	X	X	X	X	X	X		45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005 A.14.1.2 A.14.1.4	RA-3	NIST SP800-53 R3 RA-3		K.2			Commandment #1 Commandment #2 Commandment #3	CIP-007-3 - R8 - R8.1 - R8.2 - R8.3
Resiliency - Business Continuity Planning	RS-03	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for business continuity plans include the following: ・Defined purpose and scope, aligned with relevant dependencies ・Accessible to and understood by those who will use them ・Owned by a named person(s) who is responsible for their review, update and approval ・Defined lines of communication, roles and responsibilities ・Detailed recovery procedures, manual work-around and reference information ・Method for plan invocation	すべての事業継続計画が検査、保守および情報セキュリティの要求事項についての優先順位と矛盾しないように、事業継続計画立案及び計画策定に関する一貫性のある統一的な枠組みを確立し、文書化し、採用すること。事業継続計画の要求事項には以下が含まれる。 ・あらゆる依存関係と提携した、目的及び範囲の設定 ・計画の想定利用者に理解され、利用できるようにすること ・計画のレビュー、更新、承認の責任を持つ指名された人による所持 ・伝達経路、役割及び責任の定義付け ・詳細な復旧手順、手動の回避策及び参考情報 ・計画発動の方法		X	X	X	X	X	X	X	X	X	X	X	X		45 CFR 164.308 (a)(7)(ii) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308 (a)(7)(ii)(E) 45 CFR 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	CP-1 CP-2 CP-3 CP-4 CP-6 CP-7 CP-8 CP-9 CP-10 PE-17	NIST SP800-53 R3 CP-1 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) NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (3) NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-7 (1) NIST SP800-53 R3 CP-7 (2) NIST SP800-53 R3 CP-7 (3) NIST SP800-53 R3 CP-7 (5) NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 PE-17	12.9.1 12.9.3 12.9.4 12.9.6	K.1.2.3. K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15			Commandment #1 Commandment #2 Commandment #3	
Resiliency - Business Continuity Testing	RS-04	Business continuity plans shall be subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.	業務継続計画は、効果が続くことを保証するために、計画された間隔、もしくは組織的に重要なとき、もしくは、重要な組織および環境の変化に対してテストを受けなければならない。		X	X	X	X	X	X	X	X	X	X	X	X		45 CFR 164.308 (a)(7)(ii)(D)	A.14.1.5	CP-2 CP-3 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)	12.9.2	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			Commandment #1 Commandment #2 Commandment #3	
Resiliency - Environmental Risks	RS-05	Physical protection against damage from natural causes and disasters as well as deliberate attacks including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear mishap, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed and countermeasures applied.	自然損害や災害はもちろん、火事、消水、大気中の放電、太陽に誘発された地磁気嵐、風、地震、津波、爆発、原子力事故、火山活動、バイオ・ハザード、暴動、土砂崩れ、地殻変動活動、および他の自然的原因からの損害と計画的犯行といった事象からのダメージに対する物理的な保護を予測し、設計し、対策を講じなければならない。		X						X	X	X	X	X			45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii)	A.9.1.4 A.9.2.1	PE-1 PE-13 PE-14 PE-15 PE-18	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-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18		F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8	F.1	8.2.4	Commandment #1 Commandment #2 Commandment #3	CIP-004-3 R3.2
Resiliency - Equipment Location	RS-06	To reduce the risks from environmental threats, hazards and opportunities for unauthorized access equipment shall be located away from locations subject to high probability environmental risks and supplemented by redundant equipment located a reasonable distance.	装置は、環境上の脅威および災害からのリスクならびに認可されていないアクセスの機会を低減させるために、環境上のリスクが高確率で存在するところからは遠ざけ、また、妥当な距離に位置した余剰設備によって補われなければならない。		X						X	X	X	X	X			45 CFR 164.310 (c)	A.9.2.1	PE-1 PE-5 PE-14 PE-15 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	9.1.3 9.5 9.6 9.9 9.9.1	F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8	F.1		Commandment #1 Commandment #2 Commandment #3	
Resiliency - Equipment Power Failures	RS-07	Security mechanisms and redundancies shall be implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.).	セキュリティー対策と冗長化は、ユーティリティサービスの供給停止(例えば、停電、ネットワーク停止など)から設備を保護するように実装されなければならない。		X	X	X					X	X	X	X				A.9.2.2 A.9.2.3 A.9.2.4	CP-8 PE-1 PE-9 PE-10 PE-11 PE-12 PE-13 PE-14	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-11 (1) NIST SP800-53 R3 PE-12 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-14 NIST SP800-53 R3 PE-14 (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	F.1		Commandment #1 Commandment #2 Commandment #3	
Resiliency - Power / Telecommunications	RS-08	Telecommunications equipment, cabling and relays transceving data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.	データを伝送する、または支援サービスをサポートするケーブリング、およびリレー等の通信機器は、傍受または損傷から保護され、代替電力、および代替ルーティングで冗長性を持って設計されなければならない。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Telecommunications equipment, cabling and relays tranceving data or supporting services shall be protected from interception unless legally required (wire taps, etc.). These systems shall be designed with redundancies, alternative power source and alternative routing. Tenants shall have informed consent over jurisdiction of transport. 通信設備、ケーブル、データ転送、および支援サービスは、法的に必要とされない(盗聴など)限り、傍受されないように保護されている事。これらのシステムは冗長化され、代替電源および代替ルーティングを考慮し設計されている事。テナントは、管轄変更に対して告知され同意する事。	X	X						X	X	X	X				A.9.2.2 A.9.2.3	PE-1 PE-4 PE-13	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)		F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12	F.1		Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #9 Commandment #11	
Security Architecture - Customer Access Requirements	SA-01	Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access shall be addressed and remediated.	データ、資産、情報システムへのアクセスを顧客に許可する前に、顧客アクセスに関する特定されたすべてのセキュリティ、契約、規定要求事項を記述、修正しなければならない		X	X	X	X	X	X	X	X	X	X	X	X			A.6.2.1 A.6.2.2 A.11.1.1	CA-1 CA-2 CA-5 CA-6	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6		C.2.1, C.2.3, C.2.4, C.2.6.1, H.1		1.2.2 1.2.6 6.2.1 6.2.2	Commandment #6 Commandment #7 Commandment #8	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Security Architecture - User ID Credentials	SA-02	Implement and enforce (through automation) user credential and password controls for applications, databases and server and network infrastructure, requiring the following minimum standards: ・User identity verification prior to password resets. ・If password reset initiated by personnel other than user (i.e., administrator), password must be immediately changed by user upon first use. ・Timely access revocation for terminated users. ・Remove/disable inactive user accounts at least every 90 days. ・Unique user IDs and disallow group, shared, or generic accounts and passwords. ・Password expiration at least every 90 days. ・Minimum password length of at least seven (7) characters. ・Strong passwords containing both numeric and alphabetic characters. ・Allow password re-use after the last four (4) passwords used. ・User ID lockout after not more than six (6) attempts. ・User ID lockout duration to a minimum of 30 minutes or until administrator enables the user ID. ・Re-enter password to reactivate terminal after session idle time for more than 15 minutes. ・Maintain user activity logs for privileged access or access to sensitive data.	アプリケーション、データベース、サーバ、およびネットワークインフラのためのユーザクレデンシャルとパスワードは以下に要求された最低基準を(自動化して)実装しなければならない。 ・パスワード/セット前のユーザ身元証明。 ・ユーザ以外の人員(すなわち、管理者)によってパスワードリセットされた場合、ユーザは最初の使用時にすぐにパスワードを変更する。 ・無効なユーザへの即時アクセス禁止。 ・少なくとも90日間毎で不活発なユーザアカウントを取り除くか、または無効にする。 ・ユーザーIDはユニークにし、グループ利用、共有アカウント、共有パスワードを禁止する。 ・少なくとも90日間毎にパスワードを失効させる。 ・最小のパスワードの長さは少なくとも8文字。 ・数字と英字の両方を含む強いパスワード。 ・直近の4つのパスワード以外はパスワードの再利用を許容する。 ・6回ログイン失敗したらユーザIDをロックアウト。 ・ユーザIDロックアウト持続時間は最低30分か管理者が可能にするまで。 ・15分間以上のセッションアイドル時間でパスワードを再入力。 ・特権アクセスや極秘データへのアクセスはユーザの活動を記録する。				X	X	X	X			X	X	X	X	X	DS5.3 DS5.4	45 CFR 164.308(a)(5)(ii)(c) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	AC-1 AC-2 AC-3 AC-11 AU-2 AU-11 IA-1 IA-2 IA-5 IA-6 IA-8 SC-10	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-3 (3) NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 AU-2 NIST SP800-53 R3 AU-2 (3) NIST SP800-53 R3 AU-2 (4) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-2 (1) NIST SP800-53 R3 IA-2 (2) NIST SP800-53 R3 IA-2 (3) NIST SP800-53 R3 IA-2 (8) NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-5 (1) NIST SP800-53 R3 IA-5 (2) NIST SP800-53 R3 IA-5 (3) NIST SP800-53 R3 IA-5 (6) NIST SP800-53 R3 IA-5 (7) NIST SP800-53 R3 IA-6 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 SC-10	8.1 8.2, 8.3 8.4 8.5 10.1, 12.2, 12.3.8	E.6.2, E.6.3, H.1.1, H.1.2, H.2, H.3.2, H.4, H.4.1, H.4.5, H.4.8	B.1 H.5		Commandment #6 Commandment #7 Commandment #8 Commandment #9	CIP-004-3 R2.2.3 CIP-007-3 - R5.2 - R5.3.1 - R5.3.2 - R5.3.3
Security Architecture - Data Security / Integrity	SA-03	Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and leakage prevention) and integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements.	ポリシーと手順は、セキュリティ(暗号化、アクセス制御、および漏洩防止等)を確実にするために実装されたメカニズムと、1つ以上のシステム・インタフェースの間で交換されているデータの完全性により確保され、また、サードパーティの共有サービス事業者が不適当な公開、変更または破壊管理することを立法上、規定上、契約上の要件に従って防ぐことにより確保されなければならない。				X	X	X	X	X	X	X	X	X	X	DS5.11		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	AC-1 AC-4 SC-1 SC-16	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-16	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c 8.3 10.5.5 11.5	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	B.1	1.1.0 1.2.2 1.2.6 4.2.3 5.2.1 7.1.2 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	All	
Security Architecture - Application Security	SA-04	Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.	ビジネスの要求やアプリケーション規約、また、産業により受け入れられたセキュリティ標準(例えばウエブアプリケーション用のOWASP)に従って、アプリケーションは設計されなければならない。				X	X	X	X	X		X	X	X	X	AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 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	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	NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SC-6 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12)	6.5	G.16.3, I.3	I.4	1.2.6	Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11	CIP-007-3 - R5.1
Security Architecture - Data Integrity	SA-05	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 or corruption of data.	手動やシステムによる処理のエラー、データの破損を防ぐよう に、アプリケーション・インターフェースおよびデータベースにおいて、データの入出力保全ルーチンに一致しているか、編集されていないか)を実装しなければならない。				X	X	X	X	X		X	X	X	X	X		45 CFR 164.312 (c)(1) 45 CFR 164.312 (c)(2) 45 CFR 164.312(e)(2)(i)	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	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9	NIST SP800-53 R3 SI-10 NIST SP800-53 R3 SI-11 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-2 (2) NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2)	6.3.1 6.3.2	G.16.3, I.3	I.4	1.2.6	Commandment #1 Commandment #9 Commandment #11	CIP-003-3 - R4.2
Security Architecture - Production / Non-Production Environments	SA-06	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.	開発環境と非開発環境は、不正アクセスや情報資産への変更を防ぐために切り離されなければならない。		X	X	X	X	X	X		X	X	X	X		DS5.7		A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	SC-2	NIST SP800-53 R3 SC-2	6.4.1 6.4.2	I.2.7.1, I.2.20, I.2.17, I.2.22.2, I.2.22.4, I.2.22.10-14, H.1.1	B.1	1.2.6	Commandment #1 Commandment #10 Commandment #11	
Security Architecture - Remote User Multi-Factor Authentication	SA-07	Multi-factor authentication is required for all remote user access.	多要素認証がすべてのリモートユーザーアクセスに要求されなければならない。	Proposed v1.1 control revision redacted until future revision due to potential mapping impact not yet considered: Tenant authentication requirements must be met for all data access. 全てのデータアクセスに対して、テナントの認証要件を満たす事。		X	X	X	X	X		X	X	X	X	X			A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.6 A.11.7.1	AC-17 AC-20 IA-1 IA-2 MA-4	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-17 (1) NIST SP800-53 R3 AC-17 (2) NIST SP800-53 R3 AC-17 (3) NIST SP800-53 R3 AC-17 (4) NIST SP800-53 R3 AC-17 (5) NIST SP800-53 R3 AC-17 (7) NIST SP800-53 R3 AC-17 (8) NIST SP800-53 R3 AC-20 NIST SP800-53 R3 AC-20 (1) NIST SP800-53 R3 AC-20 (2) NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-2 (1) NIST SP800-53 R3 IA-2 (2) NIST SP800-53 R3 IA-2 (3) NIST SP800-53 R3 IA-2 (8) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2)	8.3	H.1.1, G.9.13, G.9.20, G.9.21	B.1	8.2.2	Commandment #6 Commandment #7 Commandment #8	CIP-004-3 R3.1
Security Architecture - Network Security	SA-08	Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.	ネットワーク環境は、信頼されているネットワークと信頼されていないネットワークの間の接続を制限するために設計、設定されるものとし、定期的に計画された間隔でレビューされなければならない。ビジネス要求に沿って実装の根拠が不確かなものも含めて、すべての使用するサービス、プロトコル、許可されたポートを記述しなければならない。 ネットワークアーキテクチャダイヤグラムは法規制に影響される可能性のある高リスク環境とデータフローを明確に特定すべきである。		X	X	X	X	X	X		X	X	X	X	X			A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	SC-7	NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	1.1 1.1.2 1.1.3 1.1.5 1.1.6 1.2 1.2.1 2.2.2 2.2.3	G.9.17, G.9.7, G.10, G 9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13	G.2 G.4 G.15 G.16 G.17 G.18 I.3	8.2.5	Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R2.2.4

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
Security Architecture - Segmentation	SA-09	System and network environments are separated by firewalls to ensure the following requirements are adhered to: ・Business and customer requirements ・Security requirements ・Compliance with legislative, regulatory, and contractual requirements ・Separation of production and non-production environments ・Preserve protection and isolation of sensitive data	システムとネットワーク環境はファイアウォールによって切り離され、以下の要件が原く守られることを保証しなければならない。 ・ビジネスと顧客の要求 ・セキュリティ要件 ・立法上、規定上、契約上の要件への準拠 ・開発環境と非開発環境の分離 ・機密データの保護と分離の維持		X	X	X	X	X	X		X	X	X	X	X	DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	AC-4 SC-2 SC-3 SC-7	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	1.1 1.2 1.2.1 1.3 1.4	G.9.2, G.9.3, G.9.13	G.17		Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R3
Security Architecture - Wireless Security	SA-10	Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following: ・Perimeter firewalls implemented and configured to restrict unauthorized traffic ・Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.). ・Logical and physical user access to wireless network devices restricted to authorized personnel ・The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	ポリシーと手順は確立されなければならない、そして、無線ネットワーク環境を保護するために以下を含んだメカニズムを実装しなければならない。 ・境界ファイアウォールを実装し、権限のないトラフィックを制限する ・ベンダー既定の設定(暗号化キー、パスワード、SNMPコミュニティ文字列など)から、強い認証や暗号化を行うセキュリティー設定。 ・認可された者以外の無線ネットワークデバイスに対する論理的、物理的アクセスの制限。 ・権限のない(凶悪な)無線ネットワークデバイスの存在を検出し、タイムリーにネットワークから分離する能力。		X	X	X	X	X	X	X	X	X	X	X	X	DS5.5 DS5.7 DS5.8 DS5.10	45 CFR 164.312 (e)(4)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) 45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(ii)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2	AC-1 AC-18 CM-6 PE-4 SC-3 SC-7	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST SP800-53 R3 AC-18 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3) NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	1.2.3 2.1.1 4.1 4.1.1 11.1 9.1.3	E.3.1, 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,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18 G.9.17, G.9.7, G.10, G.9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13	D.1 B.3 F.1 G.4 G.15 G.17 G.18	8.2.5	Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R3 CIP-007-3 - R6.1
Security Architecture - Shared Networks	SA-11	Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations.	共用ネットワークインフラシステムへのアクセスは、セキュリティポリシー、手順、および規格に従って認可された者に制限されなければならない。 外部のエンティティと共用されたネットワークは、組織間のネットワークトラフィックを切り離すために使用した防御機能が詳しく記録されたプランを持っていなければならない。		X	X	X	X	X	X	X	X	X	X	X	X		45 CFR 164.312 (a)(1)	A.10.8.1 A.11.1.1 A.11.6.2 A.11.4.6	PE-4 SC-4 SC-7	NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	1.3.5 2.4	D.1.1, E.1, F.1.1, H.1.1	B.1	8.2.5	Commandment #5 Commandment #6 Commandment #7 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R3 - R3.2
Security Architecture - Clock Synchronization	SA-12	An external accurate, externally agreed upon, time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. Note: specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organizations domicile time reference, in this event the jurisdiction or platform is treated as an explicitly defined security domain.	外部に対して正確で、外部と合意している時刻源は、組織や弱ちかに定義されたセキュリティー領域の中ですべての関連する情報処理システムの時刻を同期させるために使用し、活動しているタイムラインのトレースと再構成を行う。 注意: 特定の法管轄内、オービタルストレージ、およびリレープラットホーム(US GPS&EU(ガリレオSatellite Network)は、参照用の時計として必須である。これは、組織の場所にある参照時間と同期すること異なり、法域あるいはプラットフォームが明示的に定義されたセキュリティ領域として扱われることになる。			X	X		X			X	X	X	X		DS5.7		A.10.10.1 A.10.10.6	AU-1 AU-8	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8 NIST SP800-53 R3 AU-8 (1)	10.4	G.13, G.14.8, G.15.5, G.16.8, G.17.6, G.18.3, G.19.2.6, G.19.3.1	G.7 G.8			
Security Architecture - Equipment Identification	SA-13	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	自動化された装置識別は接続認証の方法として使用されなければならない。 位置を識別して動作を変える技術は、知られている装置位置に基づく接続認証を行うのに使用される可能性がある。		X	X	X	X	X								DS5.7		A.11.4.3	IA-3 IA-4	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-4 (4)		D.1.1, D.1.3	D.1		Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #8	
Security Architecture - Audit Logging / Intrusion Detection	SA-14	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	特権ユーザのアクセス活動、認可されているあるいは認可されていないアクセスの試み、システムの例外処理、情報セキュリティイベントを記録する監査ログは、適切なポリシーと規約に従って保持し続けなければならない。ファイル保全(ホスト)とネットワーク侵入検知(IDS)ツールは、適時検出、根本原因解析による調査、およびインシデントへの応答を容易にする。 ログを監査する物理的で論理的なユーザアクセスは認可された者に制限されなければならない。		X	X	X	X	X	X	X	X	X	X	X		DS5.5 DS5.6 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(a)(5)(ii)© 45 CFR 164.312(b)	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.2.2 A.11.5.4 A.11.6.1 A.13.1.1 A.13.2.3 A.15.2.2 A.15.1.3	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-9 AU-11 AU-12 AU-14 SI-4	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-2 NIST SP800-53 R3 AU-2 (3) NIST SP800-53 R3 AU-2 (4) NIST SP800-53 R3 AU-3 NIST SP800-53 R3 AU-3 (1) NIST SP800-53 R3 AU-4 NIST SP800-53 R3 AU-5 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-7 (1) NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-12 NIST SP800-53 R3 AU-14 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6)	10.1 10.2 10.3 10.5 10.6 10.7 11.4 12.5.2 12.9.5	G.14.7, G.14.8, G.14.9, G.14.10,G.14.11, G.14.12, G.15.5, G.15.7, G.15.8, G.16.8, G.16.9, G.16.10, G.15.9, G.17.5, G.17.7, G.17.8, G.17.6, G.17.9, G.18.2, G.18.3, G.18.5, G.18.6, G.19.2.6, G.19.3.1, G.9.6.2, G.9.6.3, G.9.6.4, G.9.19, H.2.16, H.3.3, J.1, J.2, L.5, L.9, L.10	G.7 G.8 G.9 J.1 L.2	8.2.1 8.2.2	Commandment #6 Commandment #7 Commandment #11	CIP-007-3 - R6.5
Security Architecture - Mobile Code	SA-15	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.	モバイルコードは、インストールし使用する前に認可されなければならない。また、認可されたモバイルコードが明確に定められたセキュリティ方針に従って作動することを確実にする設定を行わなければならない。すべての認可されていないモバイルコードは、実行できないようにしなければならない。			X	X		X	X		X	X	X	X	X			A.10.4.2 A.12.2.2	SC-18	NIST SP800-53 R3 SC-18 NIST SP800-53 R3 SC-18 (4)		G.20.12, I.2.5			Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification		Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability									
					Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	FedRAMP	PCI DSS v2.0	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP

QA by the HISPI
08/20/1011

