Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC					
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	2.1.2.b	ME 2.1 ME 2.2 PO 9.5 PO 9.6
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)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	11.2 11.3 6.6 12.1.2.b	DS5.5 ME2.5 ME 3.1 PO 9.6
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	2.4 12.8.2 12.8.3 12.8.4 Appendix A	ME 2.6 DS 2.1 DS 2.4
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.6.1.6 A.6.1.7	11.1.e 12.5.3 12.9	ME 3.1
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	3.1.1 3.1	ME 3.1
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.						X	X	X	X	X	X	X	X	X	X	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		

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC					
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.				X	X	X	X	X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.6.1.3 A.7.1.2 A.15.1.4		DS5.1 PO 2.3
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.				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.7.2.1	9.7.1 9.10 12.3	PO 2.3 DS 11.6
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.				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	9.5 9.6 9.7.1 9.7.2 9.10	PO 2.3 DS 11.6
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.	Control revision v1.1 rationale: Removed the specific reference to tape and disk backup as there are other media types.			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 4.3.3 A.10.5.1 A.10.7.3	3.1 3.1.1 3.2 9.9.1 9.5 9.6 10.7	DS 4.1 DS 4.2 DS 4.5 DS 4.9 DS 11.6
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.				X	X	X	X	X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.9.2.6 A.10.7.2	3.1.1 9.10 9.10.1 9.10.2 3.1	DS 11.4
Data Governance - Non-Production Data	DG-06	Production data shall not be replicated or used in non-production environments.					X	X	X	X	X	X	X	X	X			X	O	X	X	X	X	X	X	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	6.4.3	

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
Data Governance - Information Leakage	DG-07	Security mechanisms shall be implemented to prevent data leakage.				X	X	X	X	X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.10.6.2 A.12.5.4	1.2 6.5.5 11.1 11.2 11.3 11.4 A.1	DS 11.6
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				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	12.1 12.1.2	PO 9.1 PO 9.2 PO 9.4 DS 5.7
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.		X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.5.1.1 A.9.1.3 A.9.1.5	9.1 9.2 9.3 9.4	DS5.7 DS 12.1 DS 12.4 DS 4.9
Facility Security - User Access	FS-02	Physical access to information assets and functions by users and support personnel shall be restricted.		X													X	X	N				X	X	X	A.9.1.1 A.9.1.2	9,1	
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.		X						X	X	X	X	X	X			X					X	X	X	A.9.1.1	9,1	DS 12.3
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.	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.	X						X	X	X	X	X	X			X					X	X	X	A.9.1.1 A.9.1.2	9.1 9.1.1 9.1.2 9.1.3 9.2	DS 12.2 DS 12.3

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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.		X	X	X	X	X	X	X	X	X	X	X	X			X					X	X	X	A.9.1.6		DS 12.3
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.		X	X	X	X			X	X	X	X	X	X			X					X	X	X	A.9.2.7 A.10.1.2	9.8 9.9	
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.	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.	X			X		X	X	X	X	X	X	X	X		X					X	X	X	A.9.2.5 A.9.2.6	9.8 9.9 9.10	
Facility Security - Asset Management	FS-08	A complete inventory of critical assets shall be maintained with ownership defined and documented.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.7.1.1 A.7.1.2	9.9.1 12.3.3 12.3.4	
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.							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.8.1.2	12.7 12.8.3	PO 7.6
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.	Control revision v1.1 rationale: Added "tenant" into scope of control specification.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.6.1.5 A.8.1.3	12.4 12.8.2	DS 2.1
Human Resources - Employment Termination	HR-03	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented and communicated.	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).							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.8.3.1		PO 7.8

				Architectural						University Systems			Cloud Service				Supplier		Higher Education Community				Entity VPC					
Control Area	Control ID	Control Specification	Control Notes	Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS	Corp Gov Relevance	UnivCloud Tenant	Univcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	12.1 12.2	R2 DS5.2 R2 DS5.5
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								X	X	X	X	X	X	X		X					X	X	X	Clause 5 A.6.1.1	12.5	DS5.1
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.								X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2	12.1 12.2	DS5.2
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	A.12.1.1 A.15.2.2	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	AI2.1 AI2.2 AI3.3 DS2.3 DS11.6

				Architectural						University Systems			Cloud Service				Supplier		Higher Education Community				Entity VPC					
Control Area	Control ID	Control Specification	Control Notes	Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS	Corp Gov Relevance	UnivCloud Tenant	UnivCloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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.	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.							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 4.2.3 f) A.5.1.2	12.1.3	DS 5.2 DS 5.4
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.								X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.8.2.3		PO 7.7
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	3.5.1 8.5.1 12.5.4	DS 5.4
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.			X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	A.11.2.1 A.11.2.2 A.11.4.1 A 11.4.2 A.11.6.1	7.1 7.1.1 7.1.2 7.1.3 7.2.1 7.2.2 8.5.1 12.5.4	DS5.4
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.		X	X	X	X	X	X	X	X	X	X	X	X			X	O	X	X	X	X	X	X	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	8.5.4 8.5.5	DS 5.4

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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.	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.	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	A.11.2.4		DS5.3 DS5.4
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.	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.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 5.2.2 A.8.2.2	12.6 12.6.1 12.6.2	PO 7.4
Information Security - Industry Knowledge / Benchmarking	IS-12	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.								X	X	X	X	X	X	X	X	X	N				X	X	X	A.6.1.7		
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1		DS5.1
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.								X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 5.2.2 A.8.2.1 A.8.2.2 A 11.2.4 A.15.2.1	12.6.1 12.6.2	DS5.3 DS5.4 DS5.5
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X			A.10.1.3	6.4.2	DS 5.4

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	8.5.7 12.6.1	PO 4.6
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.	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)	X					X	X	X	X	X	X	X	X	X	X	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		
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).			X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	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	2.1.1 3.4 3.4.1 4.1 4.1.1 4.2	DS5.8 DS5.10 DS5.11
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.			X		X	X	X	X	X	X	X	X	X	X		X					X	X	X	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	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	DS5.8

				Architectural						University Systems			Cloud Service				Supplier		Higher Education Community				Entity VPC					
Control Area	Control ID	Control Specification	Control Notes	Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS	Corp Gov Relevance	UnivCloud Tenant	Univcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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.			X	X	X	X		X	X	X	X	X	X	X		X					X	X	X	A.12.5.1 A.12.5.2 A.12.6.1	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	AI6.1 AI3.3 DS5.9
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.			X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	A.10.4.1	5.1 5.1.1 5.2	DS5.9
Information Security - Incident Management	IS-22	Policies and procedures shall be established to triage security related events and ensure timely and thorough incident management.	Control revision v1.1 rationale: Minor editorial correction.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 4.3.3 A.13.1.1 A.13.2.1	12.9 12.9.1 12.9.2 12.9.3 12.9.4 12.9.5 12.9.6	DS5.6
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	12.5.2 12.5.3	DS5.6
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3		DS5.6
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.13.2.2	12.9.6	DS 4.9

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
Information Security - Acceptable Use	IS-26	Policies and procedures shall be established for the acceptable use of information assets.	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.					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.7.1.3	12.3.5	DS 5.3
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.	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).	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.7.1.1 A.7.1.2 A.8.3.2		
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.			X				X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	2.1.1 4.1 4.1.1 4.2	DS 5.10 5.11
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.		X	X	X	X	X	X	X	X	X	X	X	X			X	O	X	X	X	X	X	X	A.15.3.2	10.5.5	DS 5.7
Information Security - Diagnostic / Configuration Ports Access	IS-30	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.		X				X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	9.1.2	DS5.7
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.6.2.3 A.10.6.2		DS5.10

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	Univcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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).		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	9.7 9.7.2 9.8 9.9 11.1 12.3	DS5.11 DS5.5
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.	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.			X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	Clause 4.3.3 A.12.4.3 A.15.1.3	6.4.1 6.4.2	
Information Security - Utility Programs Access	IS-34	Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	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.		X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	A.11.4.1 A 11.4.4 A.11.5.4	7.1.2	DS5.7
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.							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	ISO/IEC 27001:2005 Annex A.6.1.5	12.8.2 12.8.3 12.8.4	

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC					
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivCloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	2.4 12.8.2	DS5.11
Operations Management - Policy	OP-01	Policies and procedures shall be established and made available for all personnel to adequately support services operations role.					X	X	X	X	X	X	X	X	X	X		X					X	X	X	Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1	12.1 12.2 12.3 12.4	DS13.1

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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			X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	Clause 4.3.3 A.10.7.4	12.1 12.2 12.3 12.4	DS 9 DS 13.1
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.			X	X	X		X	X	X	X	X	X	X		X	X	N				X	X	X	A.10.3.1		DS 3
Operations Management - Equipment Maintenance	OP-04	Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	A.9.2.4		A13.3
Risk Management - Program	RI-01	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	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.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	12.1.2	PO 9.1
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).	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.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	12.1.2	PO 9.4

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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		PO 9.5
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	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	12.1.3	PO 9.6
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4	12.8.1 12.8.2 12.8.3 12.8.4	DS 2.3
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	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	6.3.2	A12 A16.1
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.			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.10.1.4 A.12.5.1 A.12.5.2	1.1.1 6.3.2 6.4 6.1	A16.1 A17.6

Cloud Controls Matrix (CCM) R1.2

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivCloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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.			X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	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	1.1.1 6.1 6.4	PO 8.1
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.			X	X	X	X	X	X	X	X	X	X	X	X	X	X	N				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	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	

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
Release Management - Unauthorized Software Installations	RM-05	Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.			X	X	X	X		X	X	X	X	X	X	X		X	O	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		
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X							Clause 4.3.2 A.14.1.1 A 14.1.4	12.9.1	PO 9.1 PO 9.2 DS 4.2
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		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	ISO/IEC 27001:2005 A.14.1.2 A 14.1.4		

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC					
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	Univcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	12.9.1 12.9.3 12.9.4 12.9.6	
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.14.1.5	12.9.2	
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.		X						X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.9.1.4 A.9.2.1		
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.		X						X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.9.2.1	9.1.3 9.5 9.6 9.9 9.9.1	
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.).		X	X	X				X	X	X	X	X	X			X	O	X	X	X	X	X	X	A.9.2.2 A.9.2.3 A 9.2.4		

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC					
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivIcloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
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.	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.	X	X					X	X	X	X	X	X			X	O	X	X	X	X	X	X	A.9.2.2 A.9.2.3		
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	A.6.2.1 A.6.2.2 A.11.1.1		
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.			X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	8.1 8.2, 8.3 8.4 8.5 10.1, 12.2, 12.3.8	DS5.3 DS5.4
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.			X	X	X	X	X	X	X	X	X	X	X	X		X	O	X	X	X	X	X	X	A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c 8.3 10.5.5 11.5	DS5.11

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivCloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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.			X	X	X	X	X	X	X	X	X	X	X			X	O	X	X	X	X	X	X	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	6,5	AI2.4
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.			X	X	X	X	X	X	X	X	X	X	X		X	X	O	X	X	X	X	X	X	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	6.3.1 6.3.2	
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.		X	X	X	X	X	X	X	X	X	X	X	X			X	O	X	X	X	X	X	X	A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	6.4.1 6.4.2	DS5.7

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC					
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivCloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others	ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
Security Architecture - Remote User Multi-Factor Authentication	SA-07	Multi-factor authentication is required for all remote user access.	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.		X	X	X	X	X	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	8,3	
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.		X	X	X	X	X	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	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	
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		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X				X			A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	1.1 1.2 1.2.1 1.3 1.4	DS5.10
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		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X			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	1.2.3 2.1.1 4.1 4.1.1 11.1 9.1.3	DS5.5 DS5.7 DS5.8 DS5.10

Control Area	Control ID	Control Specification	Control Notes	Architectural						University Systems			Cloud Service			Corp Gov Relevance	Supplier		Higher Education Community				Entity VPC			ISO/IEC 27001-2005	PCI DSS v2.0	COBIT 4.1
				Phys	Network	Compute	Storage	App	Data	Services	Applications	Legacy	SaaS	PaaS	IaaS		UnivCloud Tenant	UnivCloud CSP	Entity	Student	Professor	Administrative Staff	Entity Cloud	Technical Staff	Others			
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.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X			A.10.8.1 A.11.1.1 A.11.6.2 A.11.4.6	1.3.5 2.4	
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.			X	X		X		X	X	X	X	X	X			X					X			A.10.10.1 A.10.10.6	10,4	DS5.7
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.		X	X	X	X	X																		A.11.4.3		DS5.7
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.		X	X	X	X	X	X	X	X	X	X	X	X	X		X					X			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	10.1 10.2 10.3 10.5 10.6 10.7 11.4 12.5.2 12.9.5	DS5.5 DS5.6 DS9.2
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.			X	X		X	X	X	X	X	X	X	X		X	X	X				X			A.10.4.2 A.12.2.2		

QA by the HISPI
08/20/1011

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.312(b)	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	L.1, L.2, L.7, L.9, L.11		10.2.5	Commandment #1 Commandment #2 Commandment #3	
45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	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)	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
45 CFR 164.308(b)(1) 45 CFR 164.308 (b)(4)	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)	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	
	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	L1		1.2.7 10.1.1 10.2.4	Commandment #1 Commandment #2 Commandment #3	CIP-001-1a R3 - R4
	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	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	
	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.308 (a)(2)	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
	RA-2 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	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
	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)	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
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)	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	D.2.2.9		5.1.0 5.1.1 5.2.2 8.2.6	Commandment #11	CIP-003-3 - R4.1
45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	MP-6 PE-1	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4) NIST SP800-53 R3 PE-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
45 CFR 164.308(a)(4)(ii)(B)	SA-11 CM-04	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 CM-04	I.2.18		1.2.6	Commandment #9 Commandment #10 Commandment #11	CIP-003-3 - R6

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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)	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	
45 CFR 164.308(a)(1)(ii)(A) 45 CFR 164.308(a)(8)	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	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	
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)	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	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	
45 CFR 164.310(a)(1) 45 CFR 164.310(a)(2)(ii) 45 CFR 164.310(b) 45 CFR 164.310 (c) (New)	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)	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
	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 NIST SP800-53 R3 PE-6 (1) 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 - R1.6 - R1.6.1 - R2 - R2.2
	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	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

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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
45 CFR 164.310 (d)(1)	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	F.2.18	G.21	8.2.5 8.2.6	Commandment #6 Commandment #7	
45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) 45 CFR 164.310 (d)(2)(i)	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	F.2.18, F.2.19,			Commandment #4 Commandment #5 Commandment #11	
45 CFR 164.310 (d)(2)(iii)	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)	D.1.1, D.2.1. D.2.2,	D.1		Commandment #6 Commandment #7 Commandment #8	
	PS-2 PS-3	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	E.2	E.2	1.2.9	Commandment #2 Commandment #3 Commandment #6 Commandment #9	CIP-004-3 - R2.2
45 CFR 164.310(a)(1) 45 CFR 164.308(a)(4)(i)	PL-4 PS-6 PS-7	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	E.3.5	C.1	1.2.9 8.2.6	Commandment #6 Commandment #7	
45 CFR 164.308 (a)(3)(ii)(C)	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
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)	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	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
45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	CM-1 PM-1 PM-11	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	C.1		8.2.1	Commandment #3 Commandment #6	CIP-003-3 - R1 - R1.1
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)	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	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
	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)	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306€	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	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 - R3.2 - R3.3 - R1.3 R3 - R3.1 - R3.2 - R3.3
45 CFR 164.308 (a)(1)(ii)(C)	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	
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)	AC-1 IA-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 IA-1	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
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)	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	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
45 CFR 164.308(a)(3)(ii)(C)	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	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

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	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
45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	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	E.4	E.1	1.2.10 8.2.1	Commandment #3 Commandment #6	CIP-004-3 - R1 - R2 - R2.1
	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	
	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	
	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	E.4	E.1	1.1.2 8.2.1	Commandment #6 Commandment #7 Commandment #8	
45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308(a)(4)(ii)(A) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	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)	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

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.308 (a)(5)(ii)(D)	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	E.4	E.1	1.2.10 8.2.1	Commandment #5 Commandment #6 Commandment #7	
	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	
45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	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 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SC-16 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SI-8	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
45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1)	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)	L.6		8.1.1 8.2.1 8.2.5	Commandment #9 Commandment #10 Commandment #11	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.308 (a)(1)(i)(ii)(A) 45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(B)	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	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
45 CFR 164.308 (a)(5)(ii)(B)	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	G.7		8.2.2	Commandment #4 Commandment #5	CIP-007-3 - R4 - R4.1 - R4.2
45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	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	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
45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) 16 CFR 318.5 (a) 45 CFR 160.410 (a)(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	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
45 CFR 164.308 (a)(6)(ii)	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
45 CFR 164.308 (a)(1)(ii)(D)	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	J.1.2		1.2.7 1.2.10		CIP-008-3 - R1.1

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.310 (b)	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	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	
45 CFR 164.308 (a)(3)(ii)(C)	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		
45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	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)	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	
	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			8.2.1	Commandment #2 Commandment #5 Commandment #11	CIP-003-3 - R5.2
	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	H1.1, H1.2, G.9.15			Commandment #3 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8	CIP-007-3 - R2
	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.310 (d)(1)	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 (3) NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-2 (1) NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-4 (1) NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4)	G.11, G12, G.20.13, G.20.14		1.2.6 3.2.4 8.2.6	All	CIP-007-3 - R7.1
	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)	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	
	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	H.2.16			Commandment #1 Commandment #5 Commandment #6 Commandment #7	CIP-007-3 - R2.1 - R2.2 - R2.3
	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)	C.2.5		1.2.5	Commandment #6 Commandment #7 Commandment #8 Commandment #9	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
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)(i) 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)	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)	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	
	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	G.1.1		8.2.1	Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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)	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
	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	
45 CFR 164.310 (a)(2)(iv)	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
45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(B)	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	A.1, L.1	L.2	1.2.4		CIP-009-3 - R4
45 CFR 164.308 (a)(1)(ii)(A)	PL-5 RA-2 RA-3	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	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

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.308 (a)(1)(ii)(B)	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
	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	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
	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	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		
	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)	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	
45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	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)	I.2.17, I.2.20, I.2.22		1.2.6	Commandment #1 Commandment #2 Commandment #3 Commandment #11	CIP-003-3 - R6

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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	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	
	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	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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	
45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(C)	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)	K.1.2.9, K.1.2.10, K.3.1			Commandment #1 Commandment #2 Commandment #3	
45 CFR 164.308 (a)(7)(ii)(E)	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

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.308 (a)(7)(i) 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)	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	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	
45 CFR 164.308 (a)(7)(ii)(D)	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)	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	
45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii)	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
45 CFR 164.310 (c)	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	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	
	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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	
	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	
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)	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	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
	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	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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.312(e)(2)(i)	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23	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) 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-10 NIST SP800-53 R3 SC-11 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-14 NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-18 NIST SP800-53 R3 SC-18 (4) NIST SP800-53 R3 SC-20	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
45 CFR 164.312 (c)(1) 45 CFR 164.312 (c)(2) 45 CFR 164.312(e)(2)(i)	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) 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-6 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1) NIST SP800-53 R3 SI-9	G.16.3, I.3	I.4	1.2.6	Commandment #1 Commandment #9 Commandment #11	CIP-003-3 - R4.2
	SC-2	NIST SP800-53 R3 SC-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	

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
	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)	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
	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)	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
45 CFR 164.308 (a)(4)(ii)(A)	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)	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
45 CFR 164.312 (e)~~(1)~~(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) 45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(ii)	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)	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

Scope Applicability							
HIPAA / HITECH Act	NIST SP800-53 R3	FedRAMP	BITS Shared Assessments SIG v6.0	BITS Shared Assessments AUP v5.0	GAPP (Aug 2009)	Jericho Forum	NERC CIP
45 CFR 164.312 (a)(1)	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)	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
	AU-1 AU-8	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8 NIST SP800-53 R3 AU-8 (1)	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			
	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	
45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(a)(5)(ii)©	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)	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
	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	