NIST SP 800-53 Rev 4			PCI DSS v3.0		Combined Requirement
NIST Control Family	NIST SP 800-53 Control	NIST 800-53 Control Enhancements	PCI DSS Requirements		
Access Control	AC-1: Access Control Policy and Procedures		Requirement 12, Requirement 7	12.1, 12.1.1, 7.3	
	AC-2: Account Management	AC-2 (1) (2) (3) (4) (5) (12) (13)	Requirement 8	8.1.2, 8.1.3, 8.1.4, 8.7	
	AC-3: Access Enforcement				
	AC-4: Information Flow Enforcement				
	AC-5: Separation of Duties				
	AC-6: Least Privelege	AC-6 (1) (2) (3) (5) (9) (10)	Requirement 6, Requirement 7	6.5.8, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3	
	AC-7: Unsuccessful Logon Attempts		Requirement 8	8.1.6	
	AC-8: System Use Notification				
	AC-10: Concurrent Session Control				
	AC-11: Session Lock	AC-11 (1)	Requirement 8	8.1.7	
	AC-12: Session Termination		Requirement 8	8.1.8	
	AC-14: Permitted Actions without Identification or Authentication				
	AC-17: Remote Access	AC-17 (1) (2) (3) (4)	Requirement 8	8.1.5, 2.3	
	AC-18: Wireless Access	AC-18 (1) (4) (5)	Requirement 2, Requirement 4, Requirement 11	2.1.1, 4.1.1, 11.1.1	
	AC-19: Access Control for Mobile Devices	AC-19 (5)	Requirement 1	1.4	
	AC-20: Use of External Information Systems	AC-20 (1) (2)			
	AC-21: Information Sharing				
	AC-22: Publicly Accessible Content				
Awareness and Training	AT-1: Security Awareness and Training Policy and Procedures		Requirement 12	12.1, 12.1.1	
	AT-2: Security Awareness Training	AT-2 (2)	Requirement 9, Requirement 12	9.9.3, 12.6, 12.6.1, 12.6.2	
	AT-3: Role-Based Security Training				
	AT-4: Security Training Records				
Audit and Accountability	AU-1: Audit and Accountability Policy and Procedures		Requirement 10, Requirement 12	12.1, 12.1.1, 10.8	
	AU-2: Audit Events	AU-2 (3)	Requirement 10	10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7	
	AU-3: Content of Audit Records	AU-3 (1) (2)	Requirement 10	10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6	
	AU-4: Audit Storage Capacity				
	AU-5: Response to Audit Processing Failures	AU-5 (1) (2)			
	AU-6: Audit Review, Analysis, and Reporting	AU-6 (1) (3) (5) (6)	Requirement 10	10.6, 10.6.1, 10.6.2, 10.6.3	
	AU-7: Audit Reduction and Report Generation	AU-7 (1)			
	AU-8: Time Stamps	AU-8 (1)	Requirement 10	10.4, 10.4.1, 10.4.2, 10.4.3	
	AU-9: Protection of Audit Information	AU-9 (2) (3) (4)	Requirement 10	10.5,10.5.1, 10.5.2, 10.5.3, 10.5.4	
	AU-10: Non-repudiation				
	AU-11: Audit Record Retention		Requirement 10	10.7	
	AU-12: Audit Generation	AU-12 (1) (3)	Requirement 10	10.1	
Security Assessment and Authorization	CA-1: Security Assessment and Authorization Policies and Procedures		Requirement 12	12.1, 12.1.1	
	CA-2: Security Assessments	CA-2 (1) (2)			
	CA-3: System Interconnections	CA-3 (5)			
	CA-5: Plan of Action and Milestones				
	CA-6: Security Authorization				
	CA-7: Continuous Monitoring	CA-7 (1)			
	CA-8: Penetration Testing		Requirement 11	11.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4	
	CA-9: Internal System Connections				
Configuration Management	CM-1: Configuration Management Policy and Procedures		Requirement 2, Requirement 6, Requirement 12	12.1, 12.1.1, 2.5, 6.7	
	CM-2: Baseline Configuration	CM-2 (1) (2) (3) (7)	Requirement 1	1.1.7	
	CM-3: Configuration Change Control	CM-3 (1) (2)	Requirement 1, Requirement 6	1.1.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4	
	CM-4: Security Impact Analysis	CM-4 (1)			
	CM-5: Access Restrictions for Change	CM-5 (1) (2) (3)			
	CM-6: Configuration Settings	CM-6 (1) (2)	Requirement 1, Requirement 2	1.1, 2.2, 1.2.2	
	CM-7: Least Functionality	CM-7 (1) (2) (5)	Requirement 1, Requirement 2	1.1.6, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5	
	CM-8: Information System Component Inventory	CM-8 (1) (2) (3) (4) (5)	Requirement 1, Requirement 2, Requirement 9	1.1.5, 2.4, 9.7.1, 9.9.1	
	CM-9: Configuration Management Plan				
	CM-10: Software Usage Restrictions				
	CM-11: User-Installed Software				
Contingency Planning	CP-1: Contingency Planning Policy and Procedures		Requirement 12	12.1, 12.1.1	
	CP-2: Contingency Plan	CP-2 (1) (2) (3) (4) (5) (8)			
	CP-3: Contingency Training	CP-3 (1)			
	CP-4: Contingency Plan Testing	CP-4 (1) (2)			
	CP-6: Alternate Storage Site	CP-6 (1) (2) (3)			
	CP-7: Alternate Processing Site	CP-7 (1) (2) (3) (4)			
	CP-8: Telecommunications Services	CP-8 (1) (2) (3) (4)			
	CP-9: Information System Backup	CP-9 (1) (2) (3) (5)			
	CP-10: Information System Recovery and Reconstitution	CP-10 (2) (4)			
Identification and Authentication	IA-1: Identification and Authentication Policy and Procedures		Requirement 8, Requirement 12	12.1, 12.1.1, 8.1, 8.4, 8.8	
	IA-2: Identification and Authentication (Organizational Users)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)	Requirement 8	8.1.1, 8.3	
	IA-3: Device Identification and Authentication		Requirement 8	8.6	
	IA-4: Identifier Management				
	IA-5: Authenticator Management	IA-5 (1) (2) (3) (11)	Requirement 2, Requirement 6, Requirement 8	2.1, 6.3.1, 8.2, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.5	

	IA-6: Authenticator Feedback				
	IA-7: Cryptographic Module Authentication				
	IA-8: Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	Requirement 8	8.5.1	
Incident Response	IR-1: Incident Response Policy and Procedures		Requirement 12	12.1, 12.1.1	
	IR-2: Incident Response Training	IR-2 (1) (2)	Requirement 12	12.10.4	
	IR-3: Incident Response Testing	IR-3 (2)	Requirement 12	12.10.2	
	IR-4: Incident Handling	IR-4 (1) (4)	Requirement 11, Requirement 12	11.1.2, 12.10.3	
	IR-5: Incident Monitoring	IR-5 (1)	Requirement 12	12.10.5	
	IR-6: Incident Reporting	IR-6 (1)			
	IR-7: Incident Response Assistance	IR-7 (1)	Requirement 12	12.10.3	
	IR-8: Incident Response Plan	IR-8	Requirement 12	12.10, 12.10.1, 12.10.6	
Maintenance	MA-1: System Maintenance Policy and Procedures		Requirement 12	12.1, 12.1.1	
	MA-2: Controlled Maintenance	MA-2 (2)			
	MA-3: Maintenance Tools	MA-3 (1) (2) (3)			
	MA-4: Nonlocal Maintenance	MA-4 (2) (3)			
	MA-5: Maintenance Personnel	MA-5 (1)			
	MA-6: Timely Maintenance				
Media Protection	MP-1: Media Protection Policy and Procedures		Requirement 9, Requirement 12	12.1, 12.1.1, 9.10	
	MP-2: Media Access		Requirement 9	9.6, 9.7	
	MP-3: Media Marking		Requirement 9	9.6.1	
	MP-4: Media Storage		Requirement 9	9.5, 9.5.1, 9.7	
	MP-5: Media Transport	MP-5 (4)	Requirement 9	9.6.2, 9.6.3	
	MP-6: Media Sanitization	MP-6 (1) (2) (3)	Requirement 9	9.8, 9.8.1, 9.8.2	
	MP-7: Media Use	MP-7 (1)			
Physical and Environmental Protection	PE-1: Physical and Environmental Protection Policy and Procedures		Requirement 9, Requirement 12	12.1, 12.1.1, 9.10	
	PE-2: Physical Access Authorizations		Requirement 9	9.3	
	PE-3: Physical Access Control	PE-3 (1)	Requirement 9	9.1, 9.4.1	
	PE-4: Access Control for Transmission Medium		Requirement 9	9.1.2, 9.1.3	
	PE-5: Access Control for Output Devices				
	PE-6: Monitoring Physical Access	PE-6 (1) (4)	Requirement 9	9.1.1	
	PE-8: Visitor Access Records	PE-8 (1)	Requirement 9	9.2, 9.4, 9.4.2, 9.4.3, 9.4.4	
	PE-9: Power Equipment and Cabling				
	PE-10: Emergency Shutoff				
	PE-11: Emergency Power	PE-11 (1)			
	PE-12: Emergency Lighting				
	PE-13: Fire Protection	PE-13 (1) (2) (3)			
	PE-14: Temperature and Humidity Controls				
	PE-15: Water Damage Protection	PE-15 (1)			
	PE-16: Delivery and Removal				
	PE-17: Alternate Work Site				
	PE-18: Location of Information System Components		Requirement 9	9.5	
Planning	PL-1: Security Planning Policy and Procedures		Requirement 12	12.1, 12.1.1, 12.4	
	PL-2: System Security Plan	PL-2 (3)			
	PL-4: Rules of Behavior	PL-4 (1)	Requirement 12	12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4, 12.3.5, 12.3.6, 12.3.7, 12.3.8, 12.3.9, 12.3.10	
	PL-8: Information Security Architecture				
Personnel Security	PS-1: Personnel Security Policy and Procedures		Requirement 12	12.1, 12.1.1	
	PS-2: Position Risk Designation				
	PS-3: Personnel Screening		Requirement 12	12.7	
	PS-4: Personnel Termination	PS-4 (2)			
	PS-5: Personnel Transfer				
	PS-6: Access Agreements				
	PS-7: Third-Party Personnel Security				
	PS-8: Personnel Sanctions				
Risk Assessment	RA-1: Risk Assessment Policy and Procedures		Requirement 11, Requirement 12	12.1, 12.1.1, 11.6	
	RA-2: Security Categorization				
	RA-3: Risk Assessment		Requirement 12	12.2	
	RA-5: Vulnerability Scanning	RA-5 (1) (2) (4) (5)	Requirement 6, Requirement 11	6.6, 11.1, 11.2, 11.2.1, 11.2.2, 11.2.3	
System and Services Acquisition	SA-1: System and Services Acquisition Policy and Procedures		Requirement 12	12.1, 12.1.1	
	SA-2: Allocation of Resources				
	SA-3: System Development Life Cycle		Requirement 6	6.3	
	SA-4: Acquisition Process	SA-4 (1) (2) (9) (10)			
	SA-5: Information System Documentation				
	SA-8: Security Engineering Principles		Requirement 6	6.3	
	SA-9: External Information System Services	SA-9 (2)	Requirement 2, Requirement 12	2.6, 12.8, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5, 12.9	
	SA-10: Developer Configuration Management				
	SA-11: Developer Security Testing and Evaluation		Requirement 6	6.5	
	SA-12: Supply Chain Protection				
	SA-15: Development Process, Standards, and Tools				
	SA-16: Developer-Provided Training				
	SA-17: Developer Security Architecture and Design				
	SC-1: System and Communications Protection Policy and Procedures		Requirement 3, Requirement 4, Requirement 12	12.1, 12.1.1, 3.7, 4.3	
	SC-2: Application Partitioning				

System and Communications Protection	SC-3: Security Function Isolation				
	SC-4: Information in Shared Resources				
	SC-5: Denial of Service Protection				
	SC-7: Boundary Protection	SC-7 (3) (4) (5) (7) (8) (18) (21)	Requirement 1	1.1.4, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 6.6	
	SC-8: Transmission Confidentiality and Integrity	SC-8 (1)	Requirement 2, Requirement 4, Requirement 6	2.3, 4.1, 4.2, 6.5.4	
	SC-10: Network Disconnect				
	SC-12: Cryptographic Key Establishment and Management	SC-12 (1)	Requirement 3	3.4, 3.5, 3.5.1, 3.5.2, 3.5.3, 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	
	SC-13: Cryptographic Protection		Requirement 6	6.5.3	
	SC-15: Collaborative Computing Devices				
	SC-17: Public Key Infrastructure Certificates				
	SC-18: Mobile Code				
	SC-19: Voice Over Internet Protocol				
	SC-20: Secure Name /Address Resolution Service (Authoritative Source)				
	SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver)				
	SC-22: Architecture and Provisioning for Name/Address Resolution Service				
	SC-23: Session Authenticity		Requirement 6	6.5.10	
	SC-24: Fail in Known State				
	SC-28: Protection of Information at Rest		Requirement 1, Requirement 3	1.2.2, 3.4	
	SC-39: Process Isolation				
System and Information Integrity	SI-1: System and Information Integrity Policy and Procedures		Requirement 1, Requirement 5, Requirement 11, Requirement 12	12.1, 12.1.1, 1.5, 5.4, 11.6	
	SI-2: Flaw Remediation	SI-2 (1) (2)	Requirement 5, Requirement 6	5.1.2, 6.1, 6.2, 6.4.5, 6.4.5.1, 6.4.5.2, 6.4.5.3, 6.4.5.4, 6.5.6	
	SI-3: Malicious Code Protection	SI-3 (1) (2)	Requirement 5	5.1, 5.1.1, 5.2, 5.3	
	SI-4: Information System Monitoring	SI-4 (2) (4) (5)	Requirement 11	11.4	
	SI-5: Security Alerts, Advisories, and Directives	SI-5 (1)			
	SI-6: Security Function Verification				
	SI-7: Software, Firmware, and Information Integrity	SI-7 (1) (2) (5) (7) (14)	Requirement 10, Requirement 11	10.5.5, 11.5, 11.5.1	
	SI-8: Spam Protection	SI-8 (1) (2)			
	SI-10: Information Input Validation		Requirement 6	6.5.1, 6.5.7	
	SI-11: Error Handling		Requirement 6	6.5.5	
	SI-12: Information Handling and Retention		Requirement 3	3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.3	
	SI-16: Memory Protection				