Payment Card Industry (PCI)

Data Security Standard

Summary of Changes from PCI DSS Version 1.2.1 to 2.0

October 2010

Section or Requirement		Change	Type[i]
Old	New		
General	General	**Throughout** Removed specific references to the Glossary as references are generally not provided for other glossary terms.	Clarification
General	General	**Attestations of Compliance** ▪ Attestations of Compliance removed from appendices and separate documents created. ▪ References and Appendix titles updated accordingly throughout document.	Clarification
General	General	**Introduction and PCI Data Security Standard Overview** ▪ Added information about the role of PCI DSS in the protection of cardholder data. ▪ Updated 'High Level Overview' graphic to reflect requirement titles. ▪ Clarified that the PCI DSS is an assessment tool for use during compliance assessments. ▪ Added information about resources available on the PCI SSC website.	Additional Guidance
General	General	**PCI DSS Applicability Information** ▪ Added term *"account data"* to align with PTS Secure Exchange and Reading of Data (SRED) module. ▪ Provided more details on *"cardholder data"* and *"sensitive authentication data."* ▪ Clarified that primary account data (PAN) is the defining factor for the applicability of PCI DSS. ▪ Removed footnote addressing other legislation and replaced with updated paragraph text. ▪ Updated paragraph text and applicability table to clarify which data elements must be rendered unreadable according to PCI DSS Requirement 3.4.	Clarification
N/A	General	**Relationship between PCI DSS and PA-DSS** ▪ Added new section to reflect content in PA-DSS. ▪ Clarified that use of a PA-DSS compliant application alone does not make an entity PCI DSS compliant.	Additional Guidance

Section or Requirement		Change	Type[i]
Old	New		
General	General	**Scope of Assessment for Compliance with PCI DSS Requirements** - Added *"virtualization components"* to the definition of *"system components."* - Clarified that the cardholder data environment is comprised of *"people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data."*	Additional Guidance
General	General	**Scope of Assessment for Compliance with PCI DSS Requirements** Added detailed paragraph to clarify that the first step of a PCI DSS review is to accurately determine the scope of the assessment, by identifying all locations and flows of cardholder data and ensuring that all such locations are included in the assessment.	Additional Guidance
General	General	**Network Segmentation** - Added clarifications including that segmentation may be achieved through physical or logical means. - Minor replacements to some wording to clarify meaning.	Clarification
General	General	**Wireless** Clarified focus on presence of a WLAN rather than a LAN.	Clarification
General	General	**Third Parties/Outsourcing** Minor changes to terminology for consistency.	Clarification
General	General	**Sampling of Business Facilities and System Components** - Clarified that sampling is conducted independently by the assessor and that sampling must first be performed for business facilities and then for system components within each selected facility. - Clarified that sampling does not reduce the scope of the cardholder data environment or the applicability of PCI DSS, and that sampling of the individual PCI DSS requirements is not permitted. - Clarified specific criteria that assessors must document when using sampling. Added criteria that assessors must revalidate the sampling rationale for each assessment.	Additional Guidance

Section or Requirement		Change	Type[i]
Old	New		
General	General	**Instructions and Content for Report on Compliance** ▪ Added criteria for assessor to report how the accuracy of the PCI DSS scope was validated for the assessment, in part 2. ▪ Updated reporting detail for sampling rationale and validation of sample size in part 2, to align with clarified content in Sampling section. ▪ Clarified in part 3 that list of individuals interviewed should include their organizations and topics covered. ▪ Moved *"Timeframe of Assessment"* from Part 2 to part 4, and added that the timeframe should indicate the duration and specify the time period over which the assessment occurred. ▪ Changed *"PCI DSS Security Scanning Procedures"* to *"Approved Scanning Vendors Program Guide"* in Part 5. ▪ Added explanation for N/A responses in Part 6. ▪ Minor wording changes for consistency.	Additional Guidance
General	General	**PCI DSS Compliance – Completion Steps** Updated reference to Attestations of Compliance on the PCI SSC website.	Clarification
General	General	**Detailed PCI DSS Requirements and Security Assessment Procedures** Added clarification that N/A responses are to be reported in the *"In Place"* column.	Clarification
1	1	**Introductory Paragraph** ▪ Minor wording changes for consistency. ▪ Added explanation that other system components providing firewall functionality must be treated in accordance with Requirement 1.	Additional Guidance
1.1.3	1.1.3.a, 1.1.3.b	**Testing Procedures** Separated Testing Procedure 1.1.3 into individual Testing Procedures 1.1.3.a through 1.1.3.b.	Clarification
1.1.5	1.1.5	**Requirement** Added examples of insecure services, protocols or ports.	Additional Guidance
1.2	1.2	**Requirement** Updated requirement to align with testing procedure.	Clarification
1.3	1.3	**Testing Procedure** Restructured to clarify intent of procedure.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
1.3.1	1.3.1	**Requirement and Testing Procedure** Clarified intent of requirement for DMZ to restrict inbound traffic to system components that provide authorized services, protocols, and ports.	Clarification
1.3.3	1.3.3	**Requirement and Testing Procedure** Clarified that direct connections should not be permitted between the Internet and internal networks.	Clarification
1.3.5	1.3.5	**Requirement and Testing Procedure** Clarified intent that only authorized outbound traffic is permitted.	Clarification
1.3.6	1.3.6	**Testing Procedure** Allowed greater flexibility in testing procedure by removing specification of port scanner use.	Clarification
1.3.7	1.3.7	**Requirement and Testing Procedure** Clarified that requirement applies to any type of cardholder data storage, rather than just databases.	Clarification
1.3.8	1.3.8.a – 1.3.8.b	**Requirement and Testing Procedure** ▪ Clarified intent to prevent disclosure of private IP addresses to the Internet and ensure that any such disclosure to external entities is authorized. ▪ Removed specific references to IP masquerading and use of network address translation (NAT) technologies and added examples of methods for preventing private IP address disclosure. ▪ Separated testing procedure into two sub-procedures.	Additional Guidance
1.4.b	1.4.b	**Testing Procedure** Clarified that personal firewall software should not be alterable by employee-owned computer users to align testing procedure with requirement.	Clarification
2.1	2.1	**Requirement** Minor wording changes for clarity.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
2.1.1	2.1.1.a – 2.1.1.e	**Requirement and Testing Procedure** ▪ Removed content that overlapped with Requirement 4.1.1, to clarify that the intent of this requirement is to ensure that vendor defaults are changed. ▪ Separated Testing Procedure 2.1.1 into individual Testing Procedures 2.1.1a through 2.1.1.e. ▪ Removed reference to WPA, as this is no longer considered strong encryption on its own.	Clarification
2.2	2.2	**Requirement and Testing Procedures** Moved examples of system hardening standards from testing procedure to requirement and added ISO as a source for hardening standards.	Clarification
6.2.b	2.2.b	**Testing Procedure** Moved content from former Testing Procedure 6.2.b to 2.2.b to ensure that system configuration standards are updated with vulnerabilities identified in Requirement 6.2.	Clarification
2.2.b	2.2.d	**Testing Procedure** Renumbered Testing Procedure 2.2.b to 2.2.d.	Clarification
2.2.1	2.2.1	**Requirement** Updated requirement to clarify intent of *"one primary function per server"* and use of virtualization.	Additional Guidance
N/A	2.2.1.b	**Testing Procedures** ▪ New optional testing procedure for virtualization technologies. ▪ Renumbered Testing Procedure 2.2.1 to 2.2.1.a.	Additional Guidance
2.2.2	2.2.2, 2.2.2.a – 2.2.2.b	**Requirement and Testing Procedures** ▪ Clarified that only necessary and secure services, protocols, daemons, etc., are to be enabled, and security features implemented for any insecure such services, etc., with examples. ▪ Separated Testing Procedure 2.2.2 into individual Procedures 2.2.2.a and 2.2.2.b.	Clarification
2.2.4	2.2.4.a - 2.2.4.c	**Testing Procedures** Separated Testing Procedure 2.2.4 into individual Procedures 2.2.4.a through 2.2.4.c.	Clarification
2.3	2.3, 2.3.a – 2.3.c	**Requirement and Testing Procedures** ▪ Clarified that strong cryptography is required. ▪ Separated Testing Procedure 2.3 into individual Procedures 2.3.a through 2.3.c.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
3	3	**Introductory paragraph** Clarified *"unprotected PANs should not be sent using end-user messaging technologies such as e-mail and instant messaging."*	Clarification
3.1	3.1	**Requirement and Testing Procedures** Made this a more general requirement, and moved testing procedures formerly in 3.1 to new Requirement and Testing Procedure 3.1.1 (see below).	Clarification
N/A	3.1.1, 3.1.1.a – 3.1.1.e	**Requirement and Testing Procedures** ▪ Renumbered and separated former Testing Procedure 3.1 to individual Testing Procedures 3.1.1.a through 3.1.1.d. ▪ Added detail to requirement to align with testing procedures. ▪ New Testing Procedure 3.1.1.e to clarify that assessor should verify that stored data does not exceed retention requirements defined in the policy.	Clarification
3.2	3.2	**Requirement and Testing Procedures** ▪ Added note to requirement to clarify that it is permissible for issuers and companies that support issuing processing to store sensitive authentication data when there is a business justification and the data is stored securely. ▪ New Testing Procedure 3.2.a added for issuers and companies that support issuing services to verify that business justification exists if SAD is stored. ▪ Renumbered Testing Procedure formerly 3.2 to 3.2.b, and prefaced it with *"For all other entities."*	Clarification
3.2.1	3.2.1	**Requirement and Testing Procedure** Replaced *"contained in a chip"* to *"equivalent data on a chip"* for consistency.	Clarification
3.2.1 – 3.2.3	3.2.1 – 3.2.3	**Testing Procedures** Clarified testing procedures to *"examine data sources, including but not limited to the following."*	Clarification

Section or Requirement		Change	Type[i]
Old	New		
3.4	3.4	**Requirement** ▪ Clarified that requirement applies only to the PAN. ▪ Removed note about minimum account information since this has been clarified in the requirement and in the PCI DSS Applicability Table. ▪ Clarified requirements if hashing or truncation is used to render PAN unreadable. ▪ Added Note to identify risk of hashed and truncation PANs in the same environment, and that additional security controls are required to ensure that original PAN data cannot be reconstructed. ▪ Deleted note on the use of compensating controls (since compensating controls may be applicable for most PCI DSS requirements).	Clarification
3.4.d	3.4.d	**Testing Procedure** Clarified that PAN should be *"rendered unreadable or removed,"* rather than *"sanitized or removed,"* as "sanitize" is redundant with "remove."	Clarification
3.4.1.c	3.4.1.c	**Testing Procedure** Clarified note to verify that if disk encryption is not used to encrypt removable media, than other method will need to be used.	Clarification
3.5	3.5	**Requirement** ▪ Clarified that any keys used to secure cardholder data must be protected against disclosure and misuse. ▪ Added note to clarify how this requirement applies to key-encrypting keys, if used.	Clarification
3.5.1	3.5.1	**Testing Procedure** Updated testing procedure to align with requirement.	Clarification
3.5.2	3.5.2, 3.5.2.a – 3.5.2.b	**Requirement and Testing Procedures** Added testing procedure to align with requirement.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
3.6	3.6	**Requirement and Testing Procedures** ▪ Moved note from testing procedure to requirement. ▪ Clarified in Testing Procedure 3.6.b that service providers should provide key management guidance to customers covering transmission, storage, and update of customer keys (not just storage), in accordance with Sub-Requirements 3.6.1 through 3.6.8. ▪ Deleted note about secure transmission of such keys as covered in sub-requirements.	Clarification
3.6.4	3.6.4	**Requirement and Testing Procedure** ▪ Clarified that key changes are required when keys reach the end of their defined cryptoperiod, rather than *"at least annually."* ▪ Added guidance for industry best practices.	Clarification
3.6.5	3.6.5	**Requirement and Testing Procedures** ▪ Changed wording to clarify that keys should be retired or replaced when the integrity of keys has been weakened, and provided examples. ▪ Added note that if retired or replaced keys are retained, they must be securely archived and retained only for decryption or verification purposes. ▪ Added testing procedure to verify that if retired or replaced keys are retained, that they are not used for encryption operations.	Clarification
3.6.6	3.6.6	**Requirement and Testing Procedure** ▪ Clarified that *"split knowledge and dual control"* applies only to manual clear-text cryptographic key management operations. ▪ Added note to provide examples of key management operations.	Clarification
3.6.8	3.6.8	**Requirement and Testing Procedure** Clarified that key custodians should *"formally acknowledge"* their key-custodian responsibilities rather than *"sign a form."*	Clarification

Section or Requirement		Change	Type[i]
Old	New		
4.1	4.1, 4.1.a – 4.1.e	**Requirement and Testing Procedures** ▪ Included SSH as an example of a security protocol, removed examples from testing procedure. ▪ Separated Testing Procedure 4.1 into individual Testing Procedures 4.1.a through 4.1.e. ▪ Clarified in Testing Procedure 4.1.b that trusted keys and/or certificates are required for all types of transmissions, not only SSL/TLS. ▪ Clarified in procedure 4.1.c that the protocol must be implemented to use secure configurations.	Clarification
4.1.1	4.1.1	**Requirement** Updated note regarding use of WEP as of 30 June 2010.	Clarification
4.2	4.2	**Requirement and Testing Procedures** Changed wording to clarify that unprotected (rather than unencrypted) PANs should never be sent by end-user messaging technologies.	Clarification
5.2	5.2	**Requirement and Testing Procedures** Clarified that anti-virus mechanisms should be generating audit logs, rather than just being *"capable of generating"* such logs.	Clarification
6.1	6.1	**Requirements** Clarified intent to protect system components and software from known vulnerabilities.	Clarification
6.2	6.2	**Requirement and Testing Procedures** Added that in addition to identifying vulnerabilities, processes should including ranking vulnerabilities according to risk. Provided guidance on how to assign risk rankings. ***Note:** The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*	Evolving Requirement
6.3	6.3, 6.3.a – 6.3.d	**Requirement and Testing Procedures** ▪ Added types of software applications that secure development practices would apply to. ▪ Separated Testing Procedure 6.3.a into individual Testing Procedures 6.3.a through 6.3.d.	Clarification
6.3.1	N/A	**Requirements and Testing Procedures** Removed requirements and testing procedures as vulnerability testing formerly in 6.3.1 is addressed in 6.5.1 through 6.5.9.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
6.3.2 – 6.3.5	6.4.1 – 6.4.4	**Requirements and Testing Procedures** Moved requirements and testing procedures to 6.4, to clarify intent that requirements apply to test and development environments, and not just development environments.	Clarification
6.3.6 – 6.3.7	6.3.1 – 6.3.2	**Requirements and Testing Procedures** Renumbered requirements and testing procedures due to merging and/or moving of previous requirements.	Clarification
6.3.7	6.3.2	**Requirement and Testing Procedures** ▪ Removed circular reference from note. ▪ Consolidated testing procedures (formerly 6.3.7.a and 6.3.7.b) into single procedure 6.3.2.a, to combine 'internal' and 'web' applications into single procedure. ▪ Removed specific reference to web applications and OWASP Guide to consolidate secure coding requirements for applications in scope, including non-web applications. ▪ Renumbered testing procedure previously 6.3.7.c to 6.3.2.b.	Clarification
6.4	6.4	**Requirement and Testing Procedures** ▪ Clarified requirement and testing procedure apply to change control processes and procedures. ▪ Imported content from former Testing Procedure 6.3.to align with imported testing procedures formerly 6.3.2 – 6.3.5.	Clarification
6.3.4	6.4.3	**Testing Procedure** Removed wording *"or are sanitized before use"* to clarify intent.	Clarification
6.4, 6.4.a – 6.4.b	6.4.5, 6.4.5.a – 6.4.5.b	**Requirement and Testing Procedures** Updated requirement previously 6.4 to align with testing procedures previously 6.4.a – 6.4.b, to address security patches and software modifications.	Clarification
6.4.1 – 6.4.4	6.4.5.1 – 6.4.5.4	**Requirements and Testing Procedures** Renumbered to align with imported requirements and testing procedures (formerly 6.3.2 – 6.3.5).	Clarification
6.4.1	6.4.5.1	**Testing Procedure** Clarified that documentation of impact is required in the testing procedure, to align with existing requirement.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
6.4.2	6.4.5.2	**Requirement and Testing Procedure** Clarified in requirement and testing procedure that approval is needed by *"authorized parties"* rather than *"management."*	Clarification
6.4.3	6.4.5.3, 6.4.5.3.a – 6.4.5.3.b	**Requirement and Testing Procedures** ▪ Clarified intent of requirement and testing procedure formerly 6.4.3 is for *"Functionality testing to verify that changes do not adversely impact the security of the system."* ▪ Former Requirement 6.3.1 merged into new Testing Procedure 6.4.5.3.b, to address testing of custom code changes with reference to 6.5.	Clarification
6.5	6.5	**Requirement and Testing Procedures** ▪ Clarification that secure coding and prevention of vulnerabilities applies to all custom-developed application types in scope, rather than only web applications. ▪ Removed dependency on OWASP and included other industry examples SANS CWE and CERT.	Clarification
6.5.1 – 6.5.10	6.5.1 – 6.5.9	**Requirements and Testing Procedures** ▪ Vulnerabilities formerly 6.5.1 – 6.5.10 updated and combined with former Requirement 6.3.1 to reflect current guidance from CWE, CERT, and OWASP. ▪ 6.5.7 – 6.5.9 identified as vulnerabilities specific to web applications.	Clarification
N/A	6.5.6	**Requirement and Testing Procedure** Added new requirement and testing procedure to address high-risk vulnerabilities identified in Requirement 6.2. ***Note:*** *The ranking of vulnerabilities as defined in Requirement 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*	Evolving Requirement
7.1.3	7.1.3	**Requirement and Testing Procedures** Clarified requirement for documented approval by authorized parties, rather than *"a form signed by management."*	Clarification
7.2.3	7.2.3	**Requirement and Testing Procedures** Note moved from testing procedure to requirement.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
8	8	**Introductory Paragraph** Added note to align with PA-DSS Requirement 3.2, regarding applicability of unique user ID and secure authentication controls to *"user accounts within a point of sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*"	Clarification
8.2	8.2	**Requirement** Added clarification and examples authentication methods.	Clarification
8.3	8.3	**Requirement and Testing Procedure** Clarified examples of two factor authentication to include Radius *"with tokens"* and *"other technologies that support strong authentication*." Added note clarify intent of two-factor authentication.	Clarification
8.5	8.5	**Requirements and Testing Procedures** Added term *"identification."*	Clarification
8.5.2, 8.5.7, 8.5.8, 8.5.13	8.5.2, 8.5.7, 8.5.8, 8.5.13	**Requirements and Testing Procedures** Added *"authentication"* to allow for more flexibility for companies using other authentication mechanisms outside of passwords.	Clarification
8.5.3	8.5.3	**Requirement and Testing Procedures** Included *"password resets"* as requiring unique value and immediate change after first use.	Clarification
8.5.6	8.5.6, 8.5.6.a – 8.5.6.b	**Requirement and Testing Procedures** ▪ Clarified *"access"* by vendors. Updated requirement to align with testing procedure. ▪ Separated Testing Procedure 8.5.6 into individual Procedures 8.5.6.a through 8.5.6.b.	Clarification
8.5.9 – 8.5.13	8.5.9 – 8.5.13	**Testing Procedures** ▪ Clarify password management requirements for *"non-consumer users"* from a service provider perspective. ▪ Separated single testing procedure to distinguish procedure for service providers, for each requirement.	Clarification
8.5.16, 8.5.16.a	8.5.16, 8.5.16.a – 8.5.16.d	**Requirement and Testing Procedures** ▪ Clarified that restricting direct access or queries to databases applies to user access. ▪ Separated Testing Procedure 8.5.16.a into individual Testing Procedures 8.5.16.a through 8.5.16.d.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
9	9	**Introductory Paragraph** ▪ Added terms and definitions for *"onsite personnel," "visitor,"* and *"media,"* to be used throughout requirement. ▪ New term *"onsite personnel"* replaces old term *"employee"* with a new definition to clarify intent of coverage.	Clarification
9.1.1	9.1.1.a – 9.1.1.c	**Testing Procedures** ▪ Separated testing procedure formerly 9.1.1 into individual Testing Procedures 9.1.1.a through 9.1.1.c. ▪ Changed to *"video cameras and/or access control mechanisms"* in testing procedures, since video cameras are access monitoring mechanisms that may be used with access control mechanisms.	Clarification
9.1.2	9.1.2	**Requirement and Testing Procedure** Replaced *"employee"* with *"onsite personnel."* Added example of physically accessible areas.	Clarification
9.1.3	9.1.3	**Requirement and Testing Procedure** Added *"networking/communications hardware and telecommunication lines"* to the list of items for restricting physical access. These were previously included in Requirement 9.6.	Clarification
9.2, 9.2.a	9.2, 9.2.a – 9.2.b	**Requirement and Testing Procedures** ▪ Replaced *"employee"* with *"onsite personnel."* ▪ Separated Testing Procedure 9.2.a into individual Procedures 9.2.a through 9.2.b.	Clarification
9.2.b	9.2.c	**Testing Procedures** Clarified to verify that visitor badges are easily distinguished from onsite personnel.	Clarification
9.3	9.3	**Testing Procedure** Clarified that testing procedure applies to visitor controls to align with requirement.	Clarification
9.3.1	9.3.1	**Testing Procedures** Clarified procedure from attempting to gain access to ensuring that visitors are not permitted unescorted physical access to those areas.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
9.3.2	9.3.2, 9.3.2.a – 9.3.2.b	**Requirement and Testing Procedures** ▪ Replaced *"employee"* with *"onsite personnel."* ▪ Separated Testing Procedure 9.3.2 into individual Procedures 9.3.2.a through 9.3.2.b. ▪ Clarified that Testing Procedure 9.3.2.a is to verify that visitor ID badges are used and visitors are distinguishable from employees.	Clarification
9.4	9.4	**Requirement and Testing Procedures** Replaced *"employee"* with *"onsite personnel."*	Clarification
9.5	9.5.a – 9.5.b	**Testing Procedures** ▪ Separated Testing Procedure 9.5 into individual Procedures 9.5.a through 9.5.b. ▪ Clarified that Testing Procedure 9.5.a is to observe the storage location's physical security.	Clarification
9.6	9.6	**Requirement and Testing Procedure** ▪ Replaced *"paper and electronic media"* with *"all media"* as defined in the introductory paragraph. ▪ Moved *"networking, and communications hardware, telecommunication lines"* to Testing Procedure 9.1.3.	Clarification
9.7 - 9.9	9.7 - 9.9.	**Requirements and Testing Procedures** Replaced references to *"media that contain cardholder data"* with *"media"* as it is already defined in the introductory paragraph.	Clarification
9.7.1	9.7.1	**Requirement and Testing Procedure** Clarified intent is to be able to determine sensitivity of data on media.	Clarification
10.4	10.4, 10.4.1 – 10.4.3	**Requirements and Testing Procedures** ▪ Clarified that intent is to use time synchronization technology to synchronize system clocks and times, and to ensure time is properly acquired, distributed, and stored. ▪ Changed *"time synchronization"* and *"NTP"* to *"time synchronization technology"* throughout 10.4, and clarified that *"NTP"* is an example of time synchronization technology. ▪ Separated former Testing Procedures 10.4.a through 10.4.c into new sub-requirements and Testing Procedures 10.4.1 through 10.4.3 (see below).	Clarification

Section or Requirement		Change	Type[i]
Old	New		
10.4	10.4.1	**Requirement and Testing Procedures** ▪ New sub-requirement from former Testing Procedure 10.4.b, to ensure critical systems have correct and consistent time. ▪ Restructured former Testing Procedure 10.4.b into new Testing Procedures 10.4.1.a and 10.4.1.b, to cover how time is acquired and distributed.	Clarification
10.4	10.4.2	**Requirement and Testing Procedures** New Sub-Requirement and Testing Procedures 10.4.2.a and 10.4.2.b to clarify that time data is protected and changes to time settings are authorized.	Clarification
10.4.c	10.4.3	**Requirement and Testing Procedure** Restructured former 10.4.c into new sub-requirement to ensure time is received from industry-accepted sources.	Clarification
10.7.b	10.7.b	**Testing Procedures** Clarified that the test should confirm that audit log processes are in place to *"immediately restore"* log data, rather than that log data should be *"immediately available"* for analysis.	Clarification
11.1	11.1	**Requirement and Testing Procedures** ▪ Clarified that process should be in place to *"detect unauthorized wireless access points on a quarterly basis."* ▪ Added flexibility that methods used may include wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS, and that whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.	Additional Guidance
11.1.a – 11.1.c	11.1.a – 11.1.e	**Testing Procedures** ▪ Separated former Testing Procedure 11.1.a into individual Procedures 11.1.a and 11.1.c. ▪ Added new Testing Procedure 11.1.b to test that the methodology is adequate to detect unauthorized wireless access points. ▪ Renumbered former Testing Procedure 11.1.b to 11.1.d, and clarified that configuration for generating alerts to personnel applies if automatic monitoring is used. ▪ Renumbered former Testing Procedure 11.1.c to 11.1.e	Clarification

Section or Requirement		Change	Type[i]
Old	New		
11.2	11.2, 11.2.1 – 11.2.3	**Requirements and Testing Procedures** ▪ Separated and renumbered internal & external scan requirements formerly 11.2 into individual Sub-Requirements and Testing Procedures 11.2.1 through 11.2.3. ▪ Moved note from former Testing Procedure 11.2.b to Requirement 11.2 to clarify that four internal and external scans must be verified.	Clarification
11.2.a	11.2.1.a – 11.2.1.c	**Testing Procedure** ▪ Clarified that the internal scan process includes rescans until passing results are obtained, or all *"High"* vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. ▪ Clarified that internal scans should be performed by qualified parties.	Clarification
11.2.b	11.2.2.a – 11.2.2.b	**Testing Procedures** ▪ Replaced *"PCI Security Scanning Procedures"* with *"ASV Program Guide Requirements."* ▪ Clarified that ASVs are approved by the PCI Security Standards Council (PCI SSC).	Clarification
11.2.c	11.2.3.a – 11.2.3.c	**Testing Procedures** Clarified requirements for internal & external scans to include rescans until high-risk vulnerabilities are addressed, and to be performed by qualified parties.	Clarification
11.3	11.3	**Requirement and Testing Procedures** ▪ Clarified that noted exploitable vulnerabilities must be addressed. ▪ Separated Testing Procedure 11.3.a into individual Testing Procedures 11.3.a through 11.3.b.	Clarification
11.3.2	11.3.2	**Requirement and Testing Procedure** Clarified that application penetration testing should test for relevant vulnerabilities and encompass all application types in scope.	Clarification
11.4	11.4	**Requirement and Testing Procedures** Clarified that IDS/IPS monitor traffic at the perimeter and at key points inside the CDE, rather than all traffic in the CDE.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
11.5	11.5, 11.5.a – 11.5.b	**Requirement and Testing Procedure** ▪ Replaced *"software"* with *"tools"* to clarify intent that commercial software is not sole means of meeting requirement. ▪ Added Testing Procedure 11.5.b to align with existing requirement to alert personnel to unauthorized modifications and to perform critical file comparisons at least weekly.	Clarification
12	12	**Requirement Title** Replaced *"employees and contractors"* with *"all personnel."*	Clarification
12	12	**Introductory Paragraph** Replaced *"employees"* with *"personnel"* with a slightly revised definition.	Clarification
12.1	12.1	**Testing Procedures** Replaced *"employees"* with *"personnel."*	Clarification
12.1.2	12.1.2	**Requirement and Testing Procedure** ▪ Added examples of risk assessment methodologies. ▪ Clarified that test should verify risk assessment documentation.	Additional Guidance
12.1.3	12.1.3	**Requirement** Replaced *"once a year"* with *"annually."*	Clarification
12.3	12.3	**Requirement and Testing Procedure** ▪ Removed *"employee-facing"* to clarify. ▪ Added *"tablet"* to example of technologies.	Clarification
12.3.1	12.3.1	**Requirement and Testing Procedure** Replaced *"management"* with *"authorized parties."*	Clarification
12.3.4	12.3.4	**Requirement and Testing Procedure** Clarified to allow for logical labeling.	Clarification
12.3.9	12.3.9	**Requirement and Testing Procedure** Added *"business partners"* to the requirement along with *"vendors."*	Clarification
12.3.10	12.3.10, 12.3.10.a – 12.3.10.b	**Requirement and Testing Procedures** ▪ Provided flexibility to limit prohibitions to those personnel without authorization. ▪ Renumbered Testing Procedure 12.3.10 to 12.3.10.a. Added new Testing Procedure 12.3.10.b to verify that personnel with proper authorization are protecting cardholder data in accordance with PCI DSS requirements.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
12.4	12.4	**Requirements and Testing Procedures** Replaced *"employees and contractors"* with *"personnel."*	Clarification
12.6	12.6	**Requirement and Testing Procedure** Replaced *"employees"* with *"personnel."*	Clarification
12.6.1	12.6.1	**Requirement and Testing Procedures** ▪ Replaced *"employees"* with *"personnel."* ▪ Added note to provide guidance on varying methods depending on the role of personnel.	Additional Guidance
12.6.2	12.6.2	**Requirement and Testing Procedure** ▪ Replaced *"employees"* with *"personnel."* ▪ Replaced *"company"* with *"entity."*	Clarification
12.7	12.7	**Requirement and Testing Procedure** ▪ Replaced *"employees"* with *"personnel."* ▪ Moved example from testing procedure to requirement. ▪ Clarified the note in Requirement 12.7 to apply to *"potential personnel to be hired for certain positions."*	Clarification
12.8	12.8	**Testing Procedure** Replaced *"entity being assessed"* with *"entity"* for consistency.	Clarification
12.8.4	12.8.4	**Requirements and Testing Procedures** Clarified requirement to monitor the service providers' PCI DSS compliance status at least annually. Replace *"entity assessed"* to *"entity."*	Additional Guidance
12.9.1	12.9.1, 12.9.1.a – 12.9.1.b	**Testing Procedure** ▪ Added Testing Procedure 12.9.1.b to clarify that test should include verifying that documented procedures are followed. ▪ Renumber Testing Procedure 12.9.1 to 12.9.1.a.	Clarification
12.9.3	12.9.3	**Testing Procedure** Clarified that designated personnel should be available for 24/7 incident response to align with requirement.	Clarification
Appendix D	Attestation of Compliance – Merchants	**Attestation of Compliance** ▪ Removed from Appendix as separate document. ▪ Reorganized Assessor and Merchant contact information.	Clarification

Section or Requirement		Change	Type[i]
Old	New		
Appendix E	Attestation of Compliance – Service Providers	**Attestations of Compliance** ▪ Removed from Appendix as separate document. ▪ Reorganized Assessor and Service Provider contact information. ▪ Additional options provided in list of *“Services that were included in the Scope of the PCI DSS Assessment,”* and added list of services not covered by the PCI DSS assessment.	Clarification
Appendix F	Appendix D	**Segmentation and Sampling of Business Facilities/System Components** ▪ Renamed to clarify process flow for segmentation and sampling. ▪ Created separate section titles for network segmentation and sampling. ▪ Updated to align with sampling section in introduction.	Clarification

[i] **Explanations of “Type”:**

New Type	Old Type	Definition
Clarification	Clarification	Clarifies intent of requirement. Ensure that concise wording in the standards portray the desired intent of requirements.
Additional guidance	Explanatory	Explanations and/or definitions to increase understanding or provide further information on a particular topic.
Evolving Requirement	Enhancements	Changes to ensure that the standards are up to date with emerging threats and changes in the market.