



Payment Card Industry (PCI) Datensicherheitsstandard

**Änderungsübersicht von
PCI-DSS Version 1.2.1 auf 2.0.**

Oktober 2010

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Allgemeines	Allgemeines	<p>Im</p> <p>Es wurden bestimmte Verweise auf das Glossar entfernt, zumal allgemein keine Verweise auf andere Begriffe des Glossars vorhanden sind.</p>	Erläuterung
Allgemeines	Allgemeines	<p>Compliance-Bescheinigungen</p> <ul style="list-style-type: none"> ▪ Die Compliance-Bescheinigungen wurden aus den Anhängen entfernt und es wurden separate Dokumente erstellt. ▪ Die Titel der Verweise und Anhänge wurden im Dokument aktualisiert. 	Erläuterung
Allgemeines	Allgemeines	<p>Einführung und Überblick über den PCI-Datensicherheitsstandard</p> <ul style="list-style-type: none"> ▪ Zusätzliche Informationen über die Rolle des PCI-DSS beim Schutz von Karteninhaberdaten. ▪ Aktualisierte Übersichtsgrafik, um die Titel der Anforderungen zu veranschaulichen. ▪ Es wurde verdeutlicht, dass der PCI-DSS ein Bewertungstool ist, das bei Konformitätsbeurteilungen eingesetzt wird. ▪ Zusätzliche Informationen über verfügbare Ressourcen auf der Website des PCI-DSS. 	Zusätzliche Anleitung
Allgemeines	Allgemeines	<p>Informationen zur PCI-DSS-Anwendbarkeit</p> <ul style="list-style-type: none"> ▪ Es wurde entsprechend des PTS Secure Exchange and Reading of Data (SRED) Moduls der Begriff „<i>Kontoinformationen</i>“ hinzugefügt. ▪ Es wurden weitere Einzelheiten zum Thema „<i>Karteninhaberdaten</i>“ und „<i>vertrauliche Authentifizierungsdaten</i>“ hinzugefügt. ▪ Es wurde verdeutlicht, dass die Primary Account Data (PAN) den ausschlaggebenden Faktor in Bezug auf die Anwendbarkeit der PCI-DSS-Anforderungen darstellen. ▪ Es wurde eine Fußnote mit dem Hinweis auf eine andere Gesetzgebung entfernt und durch einen aktualisierten Paragraphen ersetzt. ▪ Aktualisierter Paragraph und Anwendungstabelle, um zu verdeutlichen, welche Datenelemente gemäß PCI-DSS-Anforderung 3.4 unleserlich gemacht werden müssen. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Nicht zutr.	Allgemeines	Beziehung zwischen PCI-DSS und PA-DSS <ul style="list-style-type: none"> ▪ Es wurde ein neuer Abschnitt hinzugefügt, um den Inhalt im PA-DSS widerzuspiegeln. ▪ Es wurde verdeutlicht, dass allein durch der Einsatz einer mit dem PA-DSS konformen Anwendung eine Stelle noch nicht zwangsläufig den PCI-DSS erfüllt. 	Zusätzliche Anleitung
Allgemeines	Allgemeines	Umfang der Beurteilung der Konformität mit den PCI DSS-Anforderungen <ul style="list-style-type: none"> ▪ Zu der Definition von „Systemkomponenten“ wurde der Begriff „Virtualisierungskomponenten“ hinzugefügt. ▪ Es wurde verdeutlicht, dass die Karteninhaberumgebung aus „Personen, Prozessen und Technologien, die Karteninhaberdaten oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder übertragen“, besteht. 	Zusätzliche Anleitung
Allgemeines	Allgemeines	Umfang der Beurteilung der Konformität mit PCI DSS-Anforderungen Es wurde ein weiterer ausführlicher Abschnitt hinzugefügt, um zu verdeutlichen, dass der erste Schritt bei einer PCI-DSS-Überprüfung die genaue Bestimmung des Umfangs des Prüfverfahrens sein muss, indem alle Speicherorte und Datenflüsse von Karteninhaberdaten identifiziert werden und indem Sorge getragen wird, dass all diese Dateien in der Bewertung berücksichtigt werden.	Zusätzliche Anleitung
Allgemeines	Allgemeines	Netzwerksegmentierung <ul style="list-style-type: none"> ▪ Es wurden zusätzliche Erklärungen hinzugefügt, einschließlich, dass Segmentierungen sowohl durch physische als auch durch logische Methoden erreicht werden können. ▪ Um die Bedeutung zu verdeutlichen, wurden verschiedene Begriffe durch andere ersetzt. 	Erläuterung
Allgemeines	Allgemeines	Drahtlos Es wurde erläutert, warum das Hauptaugenmerk auf ein vorhandenes WLAN anstatt eines LAN gelegt wird.	Erläuterung
Allgemeines	Allgemeines	Dritte/Outsourcing Aus Konsistenzgründen wurden kleinere Terminologieänderungen vorgenommen.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Allgemeines	Allgemeines	<p>Stichprobenkontrolle von Unternehmenseinrichtungen und Systemkomponenten</p> <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass Stichproben vom Prüfer gesammelt und zunächst für Unternehmenseinrichtungen und anschließend für Systemkomponenten innerhalb der einzelnen ausgewählten Einrichtungen festgelegt werden müssen. ▪ Es wurde verdeutlicht, dass die Stichprobenkontrolle nicht den Umfang der Karteninhaberdaten-Umgebung oder der Anwendbarkeit der PCI-DSS-Anforderungen reduziert und dass Stichprobenkontrollen für einzelne PCI-DSS-Anforderungen nicht zulässig sind. ▪ Es wurden spezifische Kriterien genannt, die Prüfer bei der Stichprobenkontrolle dokumentieren müssen. Es wurden Kriterien hinzugefügt, nach denen der Prüfer den Grund aller Stichprobenkontrollen für jede Bewertung erneut validieren muss. 	Zusätzliche Anleitung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Allgemeines	Allgemeines	Anweisungen und Inhalt des Konformitätsberichts <ul style="list-style-type: none"> ▪ In Teil 2 wurden für Prüfer zusätzliche Kriterien dazu hinzugefügt, wie die Bestätigung der Richtigkeit des PCI-DSS-Umfangs für das Prüfverfahren berichtet werden muss. ▪ In Teil 2 wurden Berichtserstattungsdetails bezüglich des Grunds der Stichprobenkontrollen sowie der Bestätigung der Stichprobengröße aktualisiert, um diese dem überarbeiteten Inhalt im Abschnitt Stichprobenkontrolle anzupassen. ▪ In Teil 3 wurde verdeutlicht, dass in der Liste der befragten Personen auch deren Unternehmen sowie die besprochenen Themen genannt werden müssen. ▪ Der Abschnitt „<i>Zeitraumen der Beurteilung</i>“ wurde von Teil 2 nach Teil 4 verschoben und es wurde hinzugefügt, dass im Zeitrahmen die Dauer und der Zeitraum, in dem die Bewertung durchgeführt wurde, angegeben werden müssen. ▪ Der Punkt „PCI DSS-Sicherheitsscanverfahren“ wurde im Teil 5 in „<i>Programmführer für zugelassene Scanninganbieter</i>“ umgeändert. ▪ Es wurde eine Erklärung für die Antworten 'Nicht zutr.' im Teil 6 hinzugefügt. ▪ Aus Konsistenzgründen wurden kleinere Formulierungsänderungen vorgenommen. 	Zusätzliche Anleitung
Allgemeines	Allgemeines	PCI DSS-Konformität – Schritte zum Ausfüllen Der Verweis auf die Konformitätsbescheinigungen auf der Website des PCI-DSS wurde aktualisiert.	Erläuterung
Allgemeines	Allgemeines	Ausführliche PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren Es wurde eine Erläuterung hinzugefügt, dass Antworten, die 'Nicht zutr.' lauten, in der Spalte „ <i>Implementiert</i> “ aufgeführt werden müssen.	Erläuterung
1	1	Einleitung <ul style="list-style-type: none"> ▪ Aus Konsistenzgründen wurden kleinere Formulierungsänderungen vorgenommen. ▪ Es wurde eine Erklärung hinzugefügt, dass andere Systemkomponenten mit Firewall-Funktionen im Sinne der Anforderung 1 gehandhabt werden müssen. 	Zusätzliche Anleitung
1.1.3	1.1.3.a, 1.1.3.b	Prüfverfahren Das Prüfverfahren 1.1.3 wurde in die Prüfverfahren 1.1.3.a bis 1.1.3.b unterteilt.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
1.1.5	1.1.5	Anforderung Zusätzliche Beispiele für unsichere Dienste, Protokolle oder Ports.	Zusätzliche Anleitung
1.2	1.2	Anforderung Die Anforderung wurde entsprechend des Prüfverfahrens aktualisiert.	Erläuterung
1.3	1.3	Prüfverfahren Umstrukturierung zur Erläuterung des Zwecks des Verfahrens.	Erläuterung
1.3.1	1.3.1	Anforderung und Prüfverfahren Es wurde der Zweck der Implementierung einer DMZ, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene Dienste, Protokolle und Ports anbieten, verdeutlicht.	Erläuterung
1.3.3	1.3.3	Anforderung und Prüfverfahren Es wurde erläutert, dass zwischen dem Internet und internen Netzwerken keine direkten Verbindungen eingerichtet werden sollten.	Erläuterung
1.3.5	1.3.5	Anforderung und Prüfverfahren Es wurde verdeutlicht, dass nur zugelassener ausgehender Datenverkehr gestattet wird.	Erläuterung
1.3.6	1.3.6	Prüfverfahren Es wurde mehr Flexibilität im Prüfverfahren eingeräumt, indem die Anwendungsspezifikation des Port-Scanners herausgenommen wurde.	Erläuterung
1.3.7	1.3.7	Anforderung und Prüfverfahren Es wurde verdeutlicht, dass die Anforderung auf alle Arten von Karteninhaberdaten-Speicher anstatt nur auf Datenbanken Anwendung findet.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
1.3.8	1.3.8.a – 1.3.8.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass der Zweck darin besteht, die Bekanntgabe privater IP-Adressen über das Internet zu vermeiden und sicherzustellen, dass jegliche Offenlegungen an externe Stellen zuvor genehmigt werden. ▪ Es wurden Verweise auf die IP-Maskierung und die Nutzung von Network Address Translation (NAT) Technologien entfernt und Beispiele von Methoden hinzugefügt, mit denen die Veröffentlichung privater IP-Adressen verhindert werden kann. ▪ Das Prüfverfahren wurde in zwei Teilverfahren unterteilt. 	Zusätzliche Anleitung
1.4.b	1.4.b	Prüfverfahren Um das Prüfverfahren der Anforderung anzupassen wurde erläutert, dass eine persönliche Firewallsoftware nicht durch Benutzer von Mitarbeitercomputern veränderbar sein darf.	Erläuterung
2.1	2.1	Anforderung Kleinere Formulierungsänderungen zur besseren Verständlichkeit.	Erläuterung
2.1.1	2.1.1.a – 2.1.1.e	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Der Inhalt, der sich mit der Anforderung 4.1.1 überschneidet, welche erklärte, dass der Zweck der Anforderung darin liegt, sicherzustellen, dass die Anbieterstandardeinstellungen geändert werden, wurde herausgenommen. ▪ Das Prüfverfahren 2.1.1 wurde in die Prüfverfahren 2.1.1.a bis 2.1.1.e unterteilt. ▪ Der Verweis auf WPA wurde entfernt, da dies allein nicht länger als starke Verschlüsselung angesehen wird. 	Erläuterung
2.2	2.2	Anforderung und Prüfverfahren Die Beispiele zu den Systemhärtungsstandards wurden vom Prüfverfahren in die Anforderung verschoben, außerdem wird nun ISO als Quelle für Systemhärtungsstandards angeführt.	Erläuterung
6.2.b	2.2.b	Prüfverfahren Der Inhalt des früheren Prüfverfahrens 6.2.b wurde in 2.2.b integriert, um sicherzustellen, dass die Systemkonfigurationsstandards entsprechend der in der Anforderung 6.2 identifizierten Schwachstellen aktualisiert werden.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
2.2.b	2.2.d	Prüfverfahren Das Prüfverfahren 2.2.b wurde in 2.2.d unnummeriert.	Erläuterung
2.2.1	2.2.1	Anforderung Die Anforderung wurde aktualisiert, um die Bedeutung von „eine primäre Funktion pro Server“ und den Einsatz der Virtualisierung zu verdeutlichen.	Zusätzliche Anleitung
Nicht zutr.	2.2.1.b	Prüfverfahren <ul style="list-style-type: none"> ▪ Neues optionales Prüfverfahren für Virtualisierungstechnologien. ▪ Das Prüfverfahren 2.2.1 wurde in 2.2.1.a unnummeriert. 	Zusätzliche Anleitung
2.2.2	2.2.2, 2.2.2.a – 2.2.2.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde anhand von Beispielen verdeutlicht, dass ausschließlich notwendige und sichere Dienste, Protokolle, Daemons usw. aktiviert werden dürfen und Sicherheitsfunktionen für sämtliche unsicheren Dienste usw. implementiert werden müssen. ▪ Das Prüfverfahren 2.2.2 wurde in die Prüfverfahren 2.2.2.a bis 2.2.2.b unterteilt. 	Erläuterung
2.2.4	2.2.4.a - 2.2.4.c	Prüfverfahren Das Prüfverfahren 2.2.4 wurde in die Prüfverfahren 2.2.4.a bis 2.2.4.c unterteilt.	Erläuterung
2.3	2.3, 2.3.a – 2.3.c	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass eine starke Kryptographie Voraussetzung ist. ▪ Das Prüfverfahren 2.3 wurde in die Prüfverfahren 2.3.a bis 2.3.c unterteilt. 	Erläuterung
3	3	Einleitung Es wurde erklärt, dass „ungeschützte PANs nicht mit Messaging-Technologien für Endanwender wie etwa E-Mails oder Instant Messaging versendet werden dürfen.“	Erläuterung
3.1	3.1	Anforderung und Prüfverfahren Diese Anforderung wurde allgemeiner gefasst und die zuvor in 3.1 aufgeführten Prüfverfahren wurden in die neue Anforderung und das Prüfverfahren 3.1.1 (siehe unten) integriert.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Nicht zutr.	3.1.1, 3.1.1.a – 3.1.1.e	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Das frühere Prüfverfahren 3.1 wurde unnummeriert und in die Prüfverfahren 3.1.1.a bis 3.1.1.d unterteilt. ▪ Zur Anpassung an die Prüfverfahren wurden zusätzliche Details bezüglich der Anforderung geliefert. ▪ Es wurde das neue Prüfverfahren 3.1.1.e eingeführt, um zu verdeutlichen, dass der Prüfer kontrollieren muss, dass die gespeicherten Daten nicht die in der Richtlinie dargelegten Aufbewahrungsanforderungen überschreiten. 	Erläuterung
3.2	3.2	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Zu der Anforderung wurde der Hinweis hinzugefügt, dass Emittenten und Unternehmen, die Ausstellungsdienste unterstützen, vertrauliche Authentifizierungsdaten speichern dürfen, wenn hierfür eine betriebliche Begründung vorliegt und die Daten sicher gespeichert werden. ▪ Es wurde das neue Prüfverfahren 3.2.a für Emittenten und Unternehmen, die Ausstellungsdienste unterstützen, hinzugefügt, um sicherzustellen, dass eine entsprechende betriebliche Begründung vorliegt, wenn vertrauliche Authentifizierungsdaten gespeichert werden. ▪ Das frühere Prüfverfahren 3.2 wurde in 3.2.b unnummeriert und mit dem Titel „Für alle anderen Einheiten“ versehen. 	Erläuterung
3.2.1	3.2.1	Anforderung und Prüfverfahren „In einem Chip“ wurde aus Konsistenzgründen in „gleichwertige Daten auf einem Chip“ geändert.	Erläuterung
3.2.1 – 3.2.3	3.2.1 – 3.2.3	Prüfverfahren Die Prüfverfahren wurden mit der Anweisung „prüfen Sie die Datenquellen, einschließlich, aber nicht beschränkt auf folgende Punkte:“ konkretisiert.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
3.4	3.4	Anforderung <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass diese Anforderung nur für die PAN gilt. ▪ Der Hinweis zu Mindestkontoinformationen wurde herausgenommen, zumal dieser Punkt bereits in der Anforderung und in der PCI-DSS-Gültigkeitstabelle erläutert wurde. ▪ Die Anforderungen, wenn Hashing- oder Abkürzungsmethoden eingesetzt werden, um die PAN unleserlich zu machen, wurden näher erklärt. ▪ Es wurde ein Hinweis hinzugefügt, dass das Risiko gehashter und abgekürzter PANs in derselben Umgebung erkannt werden muss und dass zusätzliche Sicherheitskontrollen erforderlich sind, um sicherzustellen, dass die ursprünglichen PAN-Daten nicht wiederhergestellt werden können. ▪ Es wurde ein Hinweis über den Einsatz von Kompensationskontrollen entfernt (da Kompensationskontrollen für die meisten PCI-DSS-Anforderungen gültig sind). 	Erläuterung
3.4.d	3.4.d	Prüfverfahren Es wurde verdeutlicht, dass die PAN „ <i>unleserlich gemacht oder gelöscht werden muss</i> “ anstatt sie zu „ <i>bereinigen oder zu löschen</i> “, zumal „bereinigen“ der gleiche Vorgang wie „löschen“ ist.	Erläuterung
3.4.1.c	3.4.1.c	Prüfverfahren Der Hinweis, dass, wenn keine Datenträgerverschlüsselung zur Verschlüsselung austauschbarer Datenträger eingesetzt wird, eine andere Methode eingesetzt werden muss, wurde näher erklärt.	Erläuterung
3.5	3.5	Anforderung <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass alle Schlüssel, die für den Schutz der Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch geschützt werden müssen. ▪ Es wurde ein Hinweis hinzugefügt, welcher erläutert, dass diese Anforderung gegebenenfalls auf Schlüssel zum Verschlüsseln von Schlüsseln anzuwenden ist. 	Erläuterung
3.5.1	3.5.1	Prüfverfahren Das Prüfverfahren wurde entsprechend der Anforderung aktualisiert.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
3.5.2	3.5.2, 3.5.2.a – 3.5.2.b	Anforderung und Prüfverfahren Zur Anpassung an die Anforderung wurde ein zusätzliches Prüfverfahren eingeführt.	Erläuterung
3.6	3.6	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Der Hinweis wurde vom Prüfverfahren in die Anforderung verschoben. ▪ Im Prüfverfahren 3.6.b wurde verdeutlicht, dass Dienstanbieter ihren Kunden einen Leitfaden zum Thema Schlüsselverwaltung bereitstellen müssen, in dem die Übertragung, die Speicherung und die Aktualisierung von Kundenschlüsseln (und nicht nur die Speicherung) entsprechend den Unteranforderungen 3.6.1 bis 3.6.8 abgedeckt wird. ▪ Der Hinweis zur sicheren Übertragung dieser Schlüssel wurde herausgenommen, weil dieser Punkt bereits in den Unteranforderungen angesprochen wird. 	Erläuterung
3.6.4	3.6.4	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wird erläutert, dass die Schlüssel anstatt „<i>mindestens jährlich</i>“ geändert werden sollten, sobald sie das Ende ihrer Schlüssellebensdauer erreicht haben. ▪ Zusätzliche Anleitungen für bewährte Branchenverfahren. 	Erläuterung
3.6.5	3.6.5	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurden Umformulierungen vorgenommen und Beispiele angeführt, um hervorzuheben, dass Schlüssel entweder entfernt oder ausgetauscht werden müssen, wenn ihre Integrität beeinträchtigt wurde. ▪ Es wurde ein Hinweis hinzugefügt, der besagt, dass, wenn entfernte oder ersetzte Schlüssel aufbewahrt werden, diese ausschließlich zu Entschlüsselungs- oder Verifizierungszwecken sicher archiviert und verwahrt werden dürfen. ▪ Es wurde ein zusätzliches Prüfverfahren hinzugefügt, um sicherzugehen, dass, sollten entfernte oder ersetzte Schlüssel aufbewahrt werden, diese nicht für Verschlüsselungsvorgänge eingesetzt werden. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
3.6.6	3.6.6	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass „<i>geteiltes Wissen und doppelte Kontrollen</i>“ nur bei manuellen Verwaltungsvorgängen kryptographischer Klartext-Schlüssel Anwendung finden. ▪ Es wurde ein Hinweis mit Beispielen für Schlüsselverwaltungsvorgänge hinzugefügt. 	Erläuterung
3.6.8	3.6.8	Anforderung und Prüfverfahren Es wurde dargelegt, dass Schlüsselwächter ihre entsprechenden Verantwortungen „ <i>formell bestätigen</i> “ sollten, anstatt ein „ <i>Formular zu unterzeichnen</i> “.	Erläuterung
4.1	4.1, 4.1.a – 4.1.e	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ SSH wurde als Beispiel für ein Sicherheitsprotokoll angeführt und es wurden Beispiele aus dem Prüfverfahren entnommen. ▪ Das Prüfverfahren 4.1 wurde in die Prüfverfahren 4.1.a bis 4.1.e unterteilt. ▪ Im Prüfverfahren 4.1.b wurde verdeutlicht, dass nicht nur SSL/TLS, sondern für alle Arten von Übertragungen vertraute Schlüssel und/oder Zertifikate erforderlich sind. ▪ Im Verfahren 4.1.c wurde erklärt, dass das Protokoll implementiert werden muss, um sichere Konfigurationen verwenden zu können. 	Erläuterung
4.1.1	4.1.1	Anforderung Aktualisierter Hinweis bezüglich der Nutzung von WEP ab dem 30. Juni 2010.	Erläuterung
4.2	4.2	Anforderung und Prüfverfahren Umformulierung zur näheren Erklärung, dass ungeschützte (anstatt unverschlüsselte) PANs niemals über Messaging-Technologien für Endanwender versendet werden sollten.	Erläuterung
5.2	5.2	Anforderung und Prüfverfahren Es wird gefordert, dass Antivirus-Mechanismen tatsächlich Audit-Protokolle erstellen, anstatt lediglich „ <i>in der Lage</i> “ zu sein, derartige Protokolle zu generieren.	Erläuterung
6.1	6.1	Anforderungen Die Absicht, Systemkomponenten und Software vor bekannten Schwachstellen zu schützen, wurde näher erläutert.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
6.2	6.2	<p>Anforderung und Prüfverfahren Es wurde hinzugefügt, dass zusätzlich zur Identifizierung von Schwachstellen die Prozesse auch Bewertungen der Schwachstellen entsprechend ihres Sicherheitsrisikos durchführen sollten. Es wurde ein Leitfaden über die Durchführung von Risikobewertungen bereitgestellt.</p> <p><i>Hinweis: Die in 6.2.a beschriebene Bewertung von Sicherheitslücken wird bis 30. Juni 2012 als Best Practices angesehen, danach wird sie zu einer Anforderung.</i></p>	Neue Anforderung
6.3	6.3, 6.3.a – 6.3.d	<p>Anforderung und Prüfverfahren</p> <ul style="list-style-type: none"> ▪ Es wurden Softwareanwendungstypen hinzugefügt, auf die sichere Entwicklungspraktiken Anwendung finden würden. ▪ Das Prüfverfahren 6.3.a wurde in die einzelnen Prüfverfahren 6.3.a bis 6.3.d unterteilt. 	Erläuterung
6.3.1	Nicht zutr.	<p>Anforderungen und Prüfverfahren Es wurden Anforderungen und Prüfverfahren entfernt, da die früher in 6.3.1 aufgeführten Schwachstellenüberprüfungen nun in 6.5.1 bis 6.5.9 behandelt werden.</p>	Erläuterung
6.3.2 – 6.3.5	6.4.1 – 6.4.4	<p>Anforderungen und Prüfverfahren Die Anforderungen und Prüfverfahren wurden nach 6.4 verschoben, um zu verdeutlichen, dass die Anforderungen auf Test- und Entwicklungsumgebungen anstatt nur auf Entwicklungsumgebungen Anwendung finden.</p>	Erläuterung
6.3.6 – 6.3.7	6.3.1 – 6.3.2	<p>Anforderungen und Prüfverfahren Die Anforderungen und Prüfverfahren wurden aufgrund anderer zusammengefasster und/oder verschobener Anforderungen umnummeriert.</p>	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
6.3.7	6.3.2	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Aus dem Hinweis wurde ein Zirkelbezug entfernt. ▪ Die Testverfahren (früher 6.3.7.a und 6.3.7.b) wurden zu dem Verfahren 6.3.2.a zusammengefasst, um 'interne' und 'Web'-Anwendungen in einem einzigen Verfahren zu kombinieren. ▪ Der spezifische Verweis zu Webanwendungen und zum OWASP-Handbuch wurde herausgenommen, um die sicheren Codierungsanforderungen für alle untersuchten Anwendungen, einschließlich nicht webbasierten Anwendungen, zusammenzufassen. ▪ Das frühere Prüfverfahren 6.3.7.c wurde in 6.3.2.b umnummeriert. 	Erläuterung
6.4	6.4	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass die Anforderung und die Prüfverfahren anwendbar sind, um die Kontrollprozesse und -verfahren zu ändern. ▪ Der Inhalt des früheren Prüfverfahrens 6.3 wurde importiert, um eine Angleichung an die bereits importierten früheren Prüfverfahren 6.3.2 – 6.3.5 vorzunehmen. 	Erläuterung
6.3.4	6.4.3	Prüfverfahren Die Formulierung „ <i>oder werden vor der Verwendung bereinigt</i> “ wurde herausgenommen, um den wahren Zweck in den Vordergrund zu rücken.	Erläuterung
6.4, 6.4.a – 6.4.b	6.4.5, 6.4.5.a – 6.4.5.b	Anforderung und Prüfverfahren Die zuvor unter 6.4 beschriebene Anforderung wurde aktualisiert, um sie den Verfahren, die früher unter 6.4.a – 6.4.b geführt wurden, anzupassen, mit dem Ziel somit Sicherheitspatches und Softwareüberarbeitungen anzusprechen.	Erläuterung
6.4.1 – 6.4.4	6.4.5.1 – 6.4.5.4	Anforderungen und Prüfverfahren Es wurde eine Umnummerierung entsprechend den importierten Anforderungen und Prüfverfahren (früher 6.3.2 – 6.3.5) vorgenommen.	Erläuterung
6.4.1	6.4.5.1	Prüfverfahren Es wurde verdeutlicht, dass entsprechend der vorhandenen Anforderung im Prüfverfahren die Dokumentation über die Auswirkungen vorausgesetzt wird.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
6.4.2	6.4.5.2	Anforderung und Prüfverfahren In der Anforderung und im Prüfverfahren wird konkretisiert, dass eine Genehmigung eher von „ <i>autorisierten Parteien</i> “ anstelle des „ <i>Managements</i> “ erforderlich ist.	Erläuterung
6.4.3	6.4.5.3, 6.4.5.3.a – 6.4.5.3.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde der Zweck der früheren Anforderung und des Testverfahrens 6.4.3 zum „<i>Testen der Funktionalität, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt</i>“ verdeutlicht. ▪ Die frühere Anforderung 6.3.1 wurde im neuen Prüfverfahren 6.4.5.3.b integriert, um bezugnehmend auf 6.5 die Tests benutzerspezifischer Codeänderungen zu thematisieren. 	Erläuterung
6.5	6.5	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass sichere Codierungsverfahren und Methoden zur Vermeidung von Sicherheitslücken für alle untersuchten benutzerspezifisch entwickelten Anwendungstypen anstatt nur für Webanwendungen gelten. ▪ Die Abhängigkeit zum QWASP wurde beseitigt und es wurden andere Branchenbeispiele wie SANS, CWE und CERT angeführt. 	Erläuterung
6.5.1 – 6.5.10	6.5.1 – 6.5.9	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Die früher unter 6.5.1 – 6.5.10 geführten Schwachstellen wurden aktualisiert und mit der früheren Anforderung 6.3.1 kombiniert, um sie dem aktuellen Handbuch des CWE, CERT und QWASP anzupassen. ▪ In 6.5.7 – 6.5.9 werden webanwendungsspezifische Schwachstellen genannt. 	Erläuterung
Nicht zutr.	6.5.6	Anforderung und Prüfverfahren Es wurden eine neue Anforderung und ein neues Prüfverfahren eingeführt, um sich den in der Anforderung 6.2 identifizierten risikoreichen Schwachstellen zu widmen. <i>Hinweis: Die in 6.2.a beschriebene Bewertung von Sicherheitslücken wird bis 30. Juni 2012 als Best Practices angesehen, danach wird sie zu einer Anforderung.</i>	Neue Anforderung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
7.1.3	7.1.3	Anforderung und Prüfverfahren Die Anforderung bezüglich einer dokumentierten Genehmigung durch autorisierte Parteien anstatt ein „vom Management unterschriebenes Formular“ wurde näher erläutert.	Erläuterung
7.2.3	7.2.3	Anforderung und Prüfverfahren Der Hinweis wurde vom Prüfverfahren in die Anforderung verschoben.	Erläuterung
8	8	Einleitung Es wurde im Sinne der PA-DSS-Anforderung 3.2 ein Hinweis bezüglich der Anwendbarkeit einmaliger Benutzernamen und sicherer Authentifizierungskontrollen für „Benutzerkonten mit einer Point-of-Sale-Zahlungsanwendung, die immer nur auf eine Kartenummer für eine einzige Transaktion Zugriff haben (z. B. Kassierer-Konten)“ hinzugefügt.	Erläuterung
8.2	8.2	Anforderung Die Authentifizierungsmethoden wurden näher ausgeführt und es wurden entsprechende Beispiele geliefert.	Erläuterung
8.3	8.3	Anforderung und Prüfverfahren Es wurden Beispiele von Zwei-Faktor-Authentifizierungen verdeutlicht, in denen Radius „mit Tokens“ und „anderen Technologien, die eine starke Authentifizierung unterstützen“ eingeschlossen werden soll. Es wurde ein Hinweis hinzugefügt, um den Zweck der Zwei-Faktor-Authentifizierung näher zu erläutern.	Erläuterung
8.5	8.5	Anforderungen und Prüfverfahren Es wurde der Begriff „Identifikation“ hinzugefügt.	Erläuterung
8.5.2, 8.5.7, 8.5.8, 8.5.13	8.5.2, 8.5.7, 8.5.8, 8.5.13	Anforderungen und Prüfverfahren Der Punkt „Authentifizierung“ wurde hinzugefügt, um Unternehmen, die andere Authentifizierungsmechanismen jenseits von Kennwörtern verwenden, mehr Flexibilität einzuräumen.	Erläuterung
8.5.3	8.5.3	Anforderung und Prüfverfahren Der Punkt „Zurücksetzen von Kennwörtern“ wurde hinzugefügt, da ein einmaliger Wert benötigt wird und Kennwörter nach der ersten Verwendung sofort geändert werden müssen.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
8.5.6	8.5.6, 8.5.6.a – 8.5.6.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> Es wurde der Begriff „Zugriff“ durch Anbieter verdeutlicht. Die Anforderung wurde entsprechend des Prüfverfahrens aktualisiert. Das Prüfverfahren 8.5.6 wurde in die einzelnen Verfahren 8.5.6.a bis 8.5.6.b unterteilt. 	Erläuterung
8.5.9 – 8.5.13	8.5.9 – 8.5.13	Prüfverfahren <ul style="list-style-type: none"> Die Anforderungen hinsichtlich der Kennwortverwaltung für „Benutzer, die keine Kunden sind“ wurden aus der Perspektive eines Diensteanbieters erklärt. Für sämtliche Anforderungen wurden die einzelnen Prüfverfahren getrennt, um die Unterschiede für Diensteanbieter hervorzuheben. 	Erläuterung
8.5.16, 8.5.16.a	8.5.16, 8.5.16.a – 8.5.16.d	Anforderung und Prüfverfahren <ul style="list-style-type: none"> Es wurde verdeutlicht, dass die Beschränkung des direkten Zugriffs auf oder direkte Abfragen an Datenbanken auf Benutzerrechte zutrifft. Das Prüfverfahren 8.5.16.a wurde in die einzelnen Prüfverfahren 8.5.16.a bis 8.5.16.d unterteilt. 	Erläuterung
9	9	Einleitung <ul style="list-style-type: none"> Es wurden Begriffe und Definitionen für „Mitarbeiter vor Ort“, „Besucher“ und „Medien“ hinzugefügt, da diese in der gesamten Anforderung verwendet werden. Der neue Begriff „Mitarbeiter vor Ort“ ersetzt den alten Begriff „Mitarbeiter“ mit einer neuen Definition, um die genaue Bedeutung hervorzuheben. 	Erläuterung
9.1.1	9.1.1.a – 9.1.1.c	Prüfverfahren <ul style="list-style-type: none"> Das frühere Prüfverfahren 9.1.1 wurde in die einzelnen Prüfverfahren 9.1.1.a bis 9.1.1.c unterteilt. In den Prüfverfahren wird nun der Begriff „Videokameras und/oder Kontrollsysteme“ verwendet, zumal Videokameras Kontrollsysteme sind, die in Verbindung mit anderen Kontrollsystemen eingesetzt werden können. 	Erläuterung
9.1.2	9.1.2	Anforderung und Prüfverfahren „Mitarbeiter“ wurde durch „Mitarbeiter vor Ort“ ersetzt. Es wurden Beispiele für physisch zugängliche Bereiche aufgeführt.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
9.1.3	9.1.3	Anforderung und Prüfverfahren Zu der Liste mit Elementen, deren physischer Zugriff eingeschränkt werden muss, wurden „ <i>Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen</i> “ hinzugefügt. Diese waren zuvor Bestandteil der Anforderung 9.6.	Erläuterung
9.2, 9.2.a	9.2, 9.2.a – 9.2.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ „Mitarbeiter“ wurde durch „Mitarbeiter vor Ort“ ersetzt. ▪ Das Prüfverfahren 9.2.a wurde in die einzelnen Verfahren 9.2.a bis 9.2.b unterteilt. 	Erläuterung
9.2.b	9.2.c	Prüfverfahren Es wurde hervorgehoben, dass entsprechende Ausweise Besucher deutlich von den Mitarbeitern vor Ort unterscheiden müssen.	Erläuterung
9.3	9.3	Prüfverfahren Es wurde verdeutlicht, dass die Prüfverfahren gemäß der Anforderung für Besucherkontrollen gelten.	Erläuterung
9.3.1	9.3.1	Prüfverfahren Das Verfahren wurde hinsichtlich der Zugriffsbeschaffung konkretisiert, um sicherzustellen, dass Besucher diese Bereiche nicht ohne Begleitung betreten dürfen.	Erläuterung
9.3.2	9.3.2, 9.3.2.a – 9.3.2.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ „Mitarbeiter“ wurde durch „Mitarbeiter vor Ort“ ersetzt. ▪ Das Prüfverfahren 9.3.2 wurde in die einzelnen Verfahren 9.3.2.a bis 9.3.2.b unterteilt. ▪ Es wurde verdeutlicht, dass das Prüfverfahren 9.3.2.a dazu dient, dass Besucherausweise verwendet werden und Besucher eindeutig von Mitarbeitern unterschieden werden können. 	Erläuterung
9.4	9.4	Anforderung und Prüfverfahren „Mitarbeiter“ wurde durch „Mitarbeiter vor Ort“ ersetzt.	Erläuterung
9.5	9.5.a – 9.5.b	Prüfverfahren <ul style="list-style-type: none"> ▪ Das Prüfverfahren 9.5 wurde in die einzelnen Verfahren 9.5.a bis 9.5.b unterteilt. ▪ Es wurde verdeutlicht, dass das Prüfverfahren 9.5.a dazu dient, die physische Sicherheit der Speicherstelle zu kontrollieren. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
9.6	9.6	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Wie bereits in der Einleitung erwähnt wurde der Begriff „<i>Papierdokumente und elektronische Medien</i>“ durch „<i>alle Medien</i>“ ersetzt. ▪ Der Punkt „<i>Netzwerk- und Kommunikationshardware, Telekommunikationsleitungen</i>“ wurde in das Prüfverfahren 9.1.3 verschoben. 	Erläuterung
9.7 - 9.9	9.7 - 9.9.	Anforderungen und Prüfverfahren Die Verweise zu „ <i>Medien, die Karteninhaberdaten enthalten</i> “ wurden durch Verweise zu „ <i>Medien</i> “ ersetzt, da dieser Punkt bereits in der Einleitung behandelt wurde.	Erläuterung
9.7.1	9.7.1	Anforderung und Prüfverfahren Es wurde verdeutlicht, dass der Zweck darin besteht, die Empfindlichkeit von Daten auf Datenträgern zu bestimmen.	Erläuterung
10.4	10.4, 10.4.1 – 10.4.3	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass der Zweck darin liegt, Zeitsynchronisierungstechnologien zu verwenden, um die Systemuhren- und zeiten zu synchronisieren und somit sicherzustellen, dass die korrekte Uhrzeit empfangen, verteilt und gespeichert wird. ▪ Die Begriffe „<i>Zeitsynchronisierung</i>“ und „<i>NTP</i>“ wurden in 10.4 durch „<i>Zeitsynchronisierungstechnologien</i>“ ersetzt und es wurde erklärt, dass „<i>NTP</i>“ ein Beispiel für eine Zeitsynchronisierungstechnologie ist. ▪ Die früheren Prüfverfahren 10.4.a bis 10.4.c wurden in die neuen Unteranforderungen und Prüfverfahren 10.4.1 bis 10.4.3 unterteilt (siehe unten). 	Erläuterung
10.4	10.4.1	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Aus dem früheren Prüfverfahren 10.4.b wurde eine neue Unteranforderung erstellt, um sicherzustellen, dass alle relevanten Systeme die richtige und gleichbleibende Uhrzeit anzeigen. ▪ Das frühere Prüfverfahren 10.4.b wurde in die zwei neuen Prüfverfahren 10.4.1.a und 10.4.1.b umstrukturiert, damit auch die Art und Weise, in der die Zeit empfangen und verteilt wird, abgedeckt ist. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
10.4	10.4.2	Anforderung und Prüfverfahren Es wurden eine neue Unteranforderung und die Prüfverfahren 10.4.2.a und 10.4.2.b erstellt, um zu verdeutlichen, dass Zeitdaten geschützt sind und Änderungen der Zeiteinstellungen zulässig sind.	Erläuterung
10.4.c	10.4.3	Anforderung und Prüfverfahren Der frühere Punkt 10.4.c wurde in eine neue Unteranforderung umstrukturiert, um sicherzustellen, dass die Zeitdaten von branchenweit akzeptierten Quellen empfangen werden.	Erläuterung
10.7.b	10.7.b	Prüfverfahren Es wurde verdeutlicht, dass der Test bestätigen muss, dass entsprechende Prozesse für Audit-Protokolle implementiert sind, um Protokolldaten „unverzüglich wiederherzustellen“ anstatt Protokolldaten lediglich zu Analyse Zwecken „sofort bereitzustellen“.	Erläuterung
11.1	11.1	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde festgelegt, dass ein Prozess implementiert sein muss, um „<i>vierteljährlich eventuelle nicht autorisierte Zugriffspunkte für drahtlose Netzwerke festzustellen</i>“. ▪ Es wurde mehr Flexibilität eingeräumt, damit die eingesetzten Methoden auch Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme beinhalten können und damit die eingesetzten Methoden ausreichend sind, um jegliche nicht zugelassenen Geräte zu erkennen und zu identifizieren. 	Zusätzliche Anleitung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
11.1.a – 11.1.c	11.1.a – 11.1.e	Prüfverfahren <ul style="list-style-type: none"> ▪ Das frühere Prüfverfahren 11.1.a wurde in die Prüfverfahren 11.1.a bis 11.1.c unterteilt. ▪ Es wurde das neue Prüfverfahren 11.1.b hinzugefügt, um festzustellen, ob die angewandte Methodik, um jegliche nicht autorisierten Zugriffspunkte für drahtlose Netzwerke zu erkennen, ausreichend ist. ▪ Das frühere Prüfverfahren 11.1.b wurde in 11.1.d umnummeriert und es wurde verdeutlicht, dass die Konfiguration zur Ausgabe von Warnmeldungen an das Personal nur gilt, wenn ein automatischer Überwachungsmechanismus eingesetzt wird. ▪ Das frühere Prüfverfahren 11.1.c wurde in 11.1.e umnummeriert. 	Erläuterung
11.2	11.2, 11.2.1 – 11.2.3	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Die früheren internen und externen Scananforderungen 11.2 wurden umnummeriert und in die einzelnen Unteranforderungen und Prüfverfahren 11.2.1 bis 11.2.3 unterteilt. ▪ Der Hinweis aus dem früheren Prüfverfahren 11.2.b wurde in die Anforderung 11.2 verschoben, um zu verdeutlichen, dass vier interne und externe Scans überprüft werden müssen. 	Erläuterung
11.2.a	11.2.1.a – 11.2.1.c	Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde erläutert, dass der interne Scanprozess erneute Scans vorsieht, bis der gefundene Fehler behoben wurde oder alle „<i>schwerwiegenden</i>“ Sicherheitslücken wie in der PCI-DSS-Anforderung 6.2 dargelegt gelöst wurden. ▪ Es wurde dokumentiert, dass interne Scans von qualifiziertem Personal durchgeführt werden müssen. 	Erläuterung
11.2.b	11.2.2.a – 11.2.2.b	Prüfverfahren <ul style="list-style-type: none"> ▪ Der Begriff „<i>PCI-Sicherheitsscanverfahren</i>“ wurde durch „<i>Anforderungen des ASV-Programmführers</i>“ ersetzt. ▪ Es wurde verdeutlicht, dass die ASVs vom PCI Security Standards Council (PCI SSC) zugelassen sind. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
11.2.c	11.2.3.a – 11.2.3.c	Prüfverfahren Die Anforderungen an interne und externe Scans wurden konkretisiert, damit erneute Scans von qualifiziertem Personal durchgeführt werden, bis risikoreiche Schwachstellen behoben sind.	Erläuterung
11.3	11.3	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde angegeben, dass bekannte ausnutzbare Schwachstellen korrigiert werden müssen. ▪ Das Prüfverfahren 11.3.a wurde in die Prüfverfahren 11.3.a bis 11.3.b unterteilt. 	Erläuterung
11.3.2	11.3.2	Anforderung und Prüfverfahren Es wurde eingefügt, dass Penetrationstests Anwendungen auf wesentliche Schwachstellen überprüfen und in diesen Test sämtliche Anwendungstypen einbeziehen müssen.	Erläuterung
11.4	11.4	Anforderung und Prüfverfahren Es wurde verdeutlicht, dass IDS/IPS den Datenverkehr am Netzwerkrand und an wichtigen Punkten in der CDE anstatt den gesamten Datenverkehr in der CDE überwacht.	Erläuterung
11.5	11.5, 11.5.a – 11.5.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Der Begriff „Software“ wurde durch „Tools“ ersetzt, um zu verdeutlichen, dass kommerziell vertriebene Software nicht die einzige Methode darstellt, um diese Anforderung zu erfüllen. ▪ Entsprechend der bereits vorhandenen Anforderung, das Personal über etwaige unbefugte Änderungen zu informieren und mindestens wöchentlich einen Vergleich wichtiger Dateien durchzuführen, wurde das Prüfverfahren 11.5.b hinzugefügt. 	Erläuterung
12	12	Titel der Anforderung „Mitarbeiter und Subunternehmer“ wurde durch „alle Mitarbeiter“ ersetzt.	Erläuterung
12	12	Einleitung Der Begriff „Mitarbeiter“ wurde mit einer leicht überarbeiteten Version der Definition durch „Personal“ ersetzt.	Erläuterung
12.1	12.1	Prüfverfahren „Mitarbeiter“ wurde durch „Personal“ ersetzt.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
12.1.2	12.1.2	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurden weitere Beispiele für Risikobeurteilungsmethoden hinzugefügt. ▪ Es wurde ergänzt, dass während der Überprüfung die Dokumentation zur Risikobeurteilung kontrolliert werden sollte. 	Zusätzliche Anleitung
12.1.3	12.1.3	Anforderung Der Begriff „ <i>einmal im Jahr</i> “ wurde durch „ <i>jährlich</i> “ ersetzt.	Erläuterung
12.3	12.3	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Zur Verdeutlichung wurde der Begriff „<i>(Technologien) für Mitarbeiter</i>“ entfernt. ▪ Zu den Technologiebeispielen wurde „<i>Tablet</i>“ hinzugefügt. 	Erläuterung
12.3.1	12.3.1	Anforderung und Prüfverfahren Der Begriff „ <i>Management</i> “ wurde durch „ <i>autorisierte Parteien</i> “ ersetzt.	Erläuterung
12.3.4	12.3.4	Anforderung und Prüfverfahren Es wurde verdeutlicht, dass logische Kennzeichnungen zulässig sind.	Erläuterung
12.3.9	12.3.9	Anforderung und Prüfverfahren Zusätzlich zu dem Begriff „ <i>Geschäftspartner</i> “ wurde in der Anforderung auch der Begriff „ <i>Anbieter</i> “ hinzugefügt.	Erläuterung
12.3.10	12.3.10, 12.3.10.a – 12.3.10.b	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurden flexiblere Regelungen eingeführt, um die Beschränkungen für nicht autorisiertes Personal aufzulockern. ▪ Das Prüfverfahren 12.3.10 wurde in 12.3.10.a umnummeriert. Es wurde das neue Prüfverfahren 12.3.10.b hinzugefügt, um zu überprüfen, ob das Personal mit entsprechenden Befugnissen die Karteninhaberdaten gemäß den PCI-DSS-Anforderungen schützt. 	Erläuterung
12.4	12.4	Anforderungen und Prüfverfahren „ <i>Mitarbeiter und Subunternehmer</i> “ wurde durch „ <i>Personal</i> “ ersetzt.	Erläuterung
12.6	12.6	Anforderung und Prüfverfahren „ <i>Mitarbeiter</i> “ wurde durch „ <i>Personal</i> “ ersetzt.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
12.6.1	12.6.1	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ „Mitarbeiter“ wurde durch „Personal“ ersetzt. ▪ Es wurde ein Hinweis hinzugefügt, der als Leitfaden beim Einsatz unterschiedlicher Methoden entsprechend der Funktion des jeweiligen Personals dient. 	Zusätzliche Anleitung
12.6.2	12.6.2	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ „Mitarbeiter“ wurde durch „Personal“ ersetzt. ▪ „Unternehmen“ wurde durch „Einheit“ ersetzt. 	Erläuterung
12.7	12.7	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ „Mitarbeiter“ wurde durch „Personal“ ersetzt. ▪ Das Beispiel wurde vom Prüfverfahren in die Anforderung verschoben. ▪ Es wurde konkretisiert, dass der Hinweis in der Anforderung 12.7 nur für „potentielle neue Mitarbeiter, die ausschließlich für bestimmte Positionen eingestellt werden“ gilt. 	Erläuterung
12.8	12.8	Prüfverfahren Aus Konsistenzgründen wurde der Begriff „betreffende Einheit“ durch „Einheit“ ersetzt.	Erläuterung
12.8.4	12.8.4	Anforderungen und Prüfverfahren Die Anforderung, dass der Konformitätsstatus von Dienstleistern mit dem PCI-Datensicherheitsstandard mindestens einmal jährlich überprüft werden muss, wurde näher erläutert. „Betreffende Einheit“ wurde durch „Einheit“ ersetzt.	Zusätzliche Anleitung
12.9.1	12.9.1, 12.9.1.a – 12.9.1.b	Prüfverfahren <ul style="list-style-type: none"> ▪ Das Prüfverfahren 12.9.1.b wurde hinzugefügt, um zu verdeutlichen, dass während der Überprüfung kontrolliert werden muss, ob die dokumentierten Verfahren befolgt werden. ▪ Das Prüfverfahren 12.9.1 wurde auf 12.9.1.a umnummeriert. 	Erläuterung
12.9.3	12.9.3	Prüfverfahren Es wurde angegeben, dass zur Einhaltung dieser Anforderung an 7 Tagen die Woche durchgehend spezielles Personal für eventuelle Vorfälle zur Verfügung stehen muss.	Erläuterung
Anhang D	Konformitätsbescheinigung – Händler	Compliance-Bescheinigung <ul style="list-style-type: none"> ▪ Wurde als separates Dokument aus dem Anhang herausgenommen. ▪ Die Kontaktinformationen der Prüfer und Händler wurden neu organisiert. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Anhang E	Konformitätsbescheinigung – Dienstanbieter	Compliance-Bescheinigungen <ul style="list-style-type: none"> ▪ Wurde als separates Dokument aus dem Anhang herausgenommen. ▪ Die Kontaktinformationen der Prüfer und Dienstanbieter wurden neu organisiert. ▪ Neue Optionen in der Liste „Services, die Bestandteil der PCI-DSS-Beurteilung waren“ und zusätzliche Liste von Services, die nicht in der PCI DSS-Beurteilung berücksichtigt wurden. 	Erläuterung
Anhang F	Anhang D	Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten <ul style="list-style-type: none"> ▪ Umbenennung zur Verdeutlichung des Prozessablaufes der Segmentierung und Stichprobenkontrolle. ▪ Neue separate Abschnittsüberschriften unter Segmentierung und Stichprobenkontrolle. ▪ Aktualisierung entsprechend des Abschnitts zum Thema Stichprobenkontrolle in der Einleitung. 	Erläuterung

ⁱ Erläuterung des „Typs“:

Neuer Typ	Alter Typ	Definition
Erläuterung	Erläuterung	Verdeutlicht den Zweck der Anforderung. Stellen Sie sicher, dass die Standards präzise formuliert sind und den beabsichtigten Zweck der Anforderungen darstellen.
Zusätzliche Anleitung	Erklärung	Erklärungen und/oder Definitionen, um das Verständnis zu erweitern oder um zusätzliche Informationen zu einem bestimmten Thema zu liefern.
Überarbeitete Anforderung	Verbesserungen	Änderungen, um sicherzustellen, dass die Standards auf dem neuesten Stand bezüglich neuer Bedrohungen und Veränderungen der Branche sind.