



Payment Card Industry (PCI) Datensicherheitsstandard für Zahlungsanwendungen

**Änderungsübersicht von
PA-DSS Version 1.2.1 auf 2.0**

Oktober 2010

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Allgemeines	Allgemeines	Validierungsbestätigung Die Validierungsbestätigung wurde aus dem Anhang entfernt und es wurde ein separates Dokument erstellt. Die Dokumentverweise wurden entsprechend aktualisiert.	Erläuterung
Allgemeines	Allgemeines	Zweck dieses Dokuments Es wurde ein weiterer Verweis zu zusätzlichen Quellen der Website des PCI-DSS hinzugefügt.	Zusätzliche Anleitung
Allgemeines	Allgemeines	Beziehung zwischen PCI-DSS und PA-DSS <ul style="list-style-type: none"> ▪ Es wurde ein Satz hinzugefügt, um zu verdeutlichen, dass allein durch den Einsatz einer mit dem PS-DSS konformen Anwendung eine Einheit noch nicht zwangsläufig den PCI-DSS erfüllt. ▪ Erläuterung des Begriffs Magnetstreifendaten „und/oder gleichwertige Daten auf dem Chip.“ 	Erläuterung
Allgemeines	Allgemeines	Umfang des PA-DSS Der PA-DSS gilt nicht für Zahlungsanwendungen, die ausschließlich für den Gebrauch durch einen einzigen Kunden entwickelt und verkauft wurden.	Erläuterung
Allgemeines	Allgemeines	Anwendbarkeit des PA-DSS in Zahlungsanwendungen auf Hardware-Terminals Der Abschnitt bezüglich Zahlungsanwendungen auf Hardwareterminals, die es ermöglichen, die PA-DSS-Anforderungen außerhalb der Zahlungsanwendung zu erfüllen, wurde aktualisiert, erweitert, verdeutlicht und umbenannt.	Zusätzliche Anleitung
Allgemeines	Allgemeines	Anforderungen an PA-QSAs Der Abschnitt „Der PA-QSA muss Zugriff auf ein Labor haben, in dem der Validierungsprozess stattfinden kann“ wurde vom Punkt Testlabor in den Abschnitt PA-QSA-Anforderungen verschoben.	Erläuterung
Allgemeines	Allgemeines	Testlabor Die Standorte und Anforderungen an Testlabore wurden näher erläutert, damit der PA-QSA die angemessene Installation der Laborumgebung überprüfen kann.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Allgemeines	Allgemeines	Informationen zur PCI DSS-Anwendbarkeit <ul style="list-style-type: none"> ▪ Aktualisiert im Sinne des PCI-DSS. ▪ Es wurde der Begriff „Kontoinformationen“ hinzugefügt und weitere Einzelheiten zu den „Karteninhaberdaten“ sowie „vertraulichen Authentifizierungsdaten“ zur Verfügung gestellt. ▪ Es wurde verdeutlicht, dass die Primary Account Data (PAN) den ausschlaggebenden Faktor in Bezug auf die Anwendbarkeit der PCI-DSS-Anforderungen darstellen. ▪ Es wurde ein Abschnitt hinzugefügt (die früheren Fußnoten wurden ersetzt) und eine Tabelle aktualisiert, um zu verdeutlichen, welche Datenelemente gemäß PCI-DSS-Anforderung 3.4 unleserlich gemacht werden müssen. 	Erläuterung
Allgemeines	Allgemeines	Anweisungen und Inhalt für den Validierungsbericht Im Teil 3 wurden zusätzliche Kriterien für die Berichterstattung hinzugefügt, falls eine Anforderung auf eine bestimmte Zahlungsanwendung nicht zutrifft.	Erläuterung
Allgemeines	Allgemeines	PA-DSS-Schritte zur Fertigstellung Aktualisierter Verweis zur Validierungsbestätigung.	Erläuterung
Alle Anforderungen	Alle Anforderungen	Anforderungsspalte im Standard Alle Hinweise, die zuvor „PCI-Datensicherheitsstandard-Anforderung X.X“ lauteten, wurden umformuliert in „Im Sinne der PCI-DSS-Anforderung X.X“, um die Angleichung zwischen PCI-DSS und PA-DSS hervorzuheben.	Erläuterung
Alle Anforderungen	Alle Anforderungen	Im Standard enthaltene Anforderungen und Prüfverfahren Immer wenn eine PA-DSS-Anforderung „im Sinne der PCI-DSS-Anforderung X.X“ überprüft werden sollte, wurden die jeweiligen Anforderung und die Prüfverfahren aus dem PCI-DSS importiert und entsprechend der Zahlungsanwendungen umformuliert.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
1.1	1.1	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde ein 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. ▪ Für Emittenten und Unternehmen, die Ausstellungsdienste unterstützen, wurde das Prüfverfahren 1.1.a hinzugefügt, um sicherzustellen, dass die Zahlungsanwendung ausschließlich für Emittenten und/oder Unternehmen, die Ausstellungsdienste unterstützen, gedacht ist. ▪ Das Prüfverfahren 1.1 wurde in 1.1.b umnummeriert und mit dem Titel „Für alle anderen Zahlungsanwendungen“ versehen. 	Erläuterung
1.1.1	1.1.1	Anforderung und Prüfverfahren Der Begriff „auf einem Chip“ wurde in „gleichwertige Daten auf einem Chip“ umgeändert.	Erläuterung
1.1.1 – 1.1.3	1.1.1 – 1.1.3	Anforderungen und Prüfverfahren Es wurden bestimmte Verweise auf dem Glossar herausgenommen, da im Standard auch andere Begriff ohne Verweise auf das Glossar genannt werden.	Erläuterung
1.1.1 – 1.1.3	1.1.1 – 1.1.3	Prüfverfahren Es wurde verdeutlicht, dass während den Tests auch eine Überprüfung <i>„mindestens folgender Dateitypen“ stattfinden muss.</i>	Erläuterung
2.1	2.1	Prüfverfahren Es wurde verdeutlicht, dass alle Speicherorte von Karteninhaberdaten Anweisungen zur Konfiguration der zugrundeliegenden Software beinhalten müssen, um einer unbeabsichtigten Erfassung oder Aufbewahrung der Karteninhaberdaten vorzubeugen.	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
2.3	2.3, 2.3.a – 2.3.e	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass diese Anforderung nur für die PAN Anwendung findet. ▪ Die Notiz über Mindestkontoinformationen wurde herausgenommen, zumal dieser Punkt bereits in der Anforderung und in der PCI-DSS-Gültigkeitstabelle erläutert wurde. ▪ Die Anforderungen bezüglich der Verwendung von Hashing- oder Abkürzungsmethoden, um eine PAN unleserlich zu machen, wurden näher erläutert. ▪ 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. ▪ Die Prüfverfahren wurden aus dem PCI-DSS importiert, um die neuen Verfahren 2.3.a bis 2.3.e zu erstellen. 	Erläuterung
2.4	2.4, 2.4.a – 2.4.c	Prüfverfahren Der Verweis zum PCI-DSS wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert und umformuliert, um entsprechend der Zahlungsanwendungen die neuen Verfahren 2.4.a bis 2.4.c zu erstellen.	Erläuterung
2.5	2.5, 2.5.a – 2.5.c	Anforderung und Prüfverfahren <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. ▪ Der Verweis zum PCI-DSS wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert und umformuliert, um entsprechend der Zahlungsanwendungen die neuen Verfahren 2.5.a bis 2.5.c zu erstellen. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
2.6	2.6, 2.6.1 – 2.6.7	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Der Verweis zum PCI-DSS wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert und umformuliert, um entsprechend der Zahlungsanwendungen die neuen Verfahren 2.6.1 bis 2.6.7 zu erstellen. ▪ Das Prüfverfahren 2.6.a wurde mit Unterlagen aus dem <i>PA-DSS-Implementierungshandbuch</i> ergänzt und das frühere Verfahren 2.6.a wurde in 2.6.b unnummeriert. 	Erläuterung
2.7	2.7	Anforderung und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde verdeutlicht, dass die ursprüngliche Formulierung des sicheren Löschens auf ein Tool oder einen Prozess hinweist, der kryptographische Schlüssel oder Material, das von früheren Versionen der Zahlungsanwendung gespeichert wurde, unwiderruflich löscht. ▪ Der Abschnitt „<i>Entfernung eines kryptographischen Schlüssels</i>“ wurde als Beispiel für das unwiderrufliche Löschen kryptographischer Schlüsselmaterialien oder Kryptogramme angeführt. 	Erläuterung
3.1	3.1, 3.1.1 – 3.1.10	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Der Verweis zum PCI-DSS wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert und umformuliert, um entsprechend der Zahlungsanwendungen die neuen Verfahren 3.1.1 bis 3.1.10 zu erstellen. ▪ Es wurde verdeutlicht, dass eine sichere Authentifizierung für alle Konten durchgesetzt werden muss, die von der Anwendung bei Abschluss der Installation sowie bei nachträglichen Änderungen nach der Installation generiert oder verwaltet werden. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
3.1.a – 3.1.c	3.1.a – 3.1.d	<p>Prüfverfahren</p> <ul style="list-style-type: none"> ▪ Das Prüfverfahren 3.1.c wurde nach 3.1.a verschoben, um die Dokumentation des <i>PA-DSS-Implementierungshandbuchs</i> aufzunehmen und entsprechend der importierten Unteranforderungen wurde der Inhalt näher erklärt. ▪ Das Prüfverfahren 3.1.a wurde entsprechend der importierten Unteranforderungen nach 3.1.d verschoben, und es wurden zusätzliche Erläuterungen zur Überprüfung dessen, ob bei Abschluss der Installation sowie im Falle nachträglicher Änderungen nach der Installation eine sichere Authentifizierung angewendet wird, hinzugefügt. ▪ Es wurde das neue Prüfverfahren 3.1.c hinzugefügt, um sicherzustellen, dass die Zahlungsanwendung die Änderung der Standardkonten durchsetzt. 	Erläuterung
3.2	3.2	<p>Anforderung</p> <p>Es wurde verdeutlicht, dass diese Anforderung für den Leitfaden des Anbieters, der dem Kunden ausgehändigt wird, gilt.</p>	Erläuterung
4.1	4.1, 4.1.a – 4.1.b	<p>Prüfverfahren</p> <p>Das Prüfverfahren wurde entsprechend der umstrukturierten Anforderungen von 4.2.b nach 4.1.b verschoben. Kleinere Umformulierungen zur Erläuterung.</p>	Erläuterung
4.2	4.2, 4.2.1 – 4.2.7	<p>Anforderungen und Prüfverfahren</p> <ul style="list-style-type: none"> ▪ Es wurden bestimmte Informationen näher erklärt, die in den Protokolldateien eingeschlossen werden müssen. ▪ Der Verweis zum PCI-DSS wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert und umformuliert, um entsprechend der Zahlungsanwendungen die neuen Verfahren 4.2.1 bis 4.2.7 zu erstellen. 	Erläuterung
4.2	4.3, 4.3.1 – 4.3.6	<p>Anforderungen und Prüfverfahren</p> <ul style="list-style-type: none"> ▪ Es wurden bestimmte Informationen näher erklärt, die in den Protokolldateien eingeschlossen werden müssen. ▪ Der Verweis zum PCI-DSS (zuvor unter 4.2) wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert und umformuliert, um entsprechend der Zahlungsanwendungen die neuen Unteranforderungen und Prüfverfahren 4.3.1 bis 4.3.6 zu erstellen. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
Nicht zutr.	4.4	Neue Anforderungen und Prüfverfahren Es wurde eine neue Anforderung hinzugefügt, damit die Zahlungsanwendungen gemäß der PCI-DSS-Anforderung 10.5.3 eine zentralisierte Protokollierung zulassen.	Neue Anforderung
5.1	5.1	Anforderungen und Prüfverfahren Aktualisiert im Sinne der PCI-DSS-Anforderung 6.3.	Erläuterung
5.1.1	Nicht zutr.	Anforderungen und Prüfverfahren Punkt 5.1.1 wurde herausgenommen, da Schwachstellenüberprüfungen nun in 5.2.1 bis 5.2.9 behandelt werden.	Erläuterung
5.1.2 – 5.1.3	Nicht zutr.	Anforderungen und Prüfverfahren Wurde zur besseren Verständlichkeit herausgenommen, da die Produktionsumgebung für Anwendungsentwickler hinsichtlich des PA-DSS keine Anwendung findet.	Erläuterung
5.1.1 – 5.1.7	5.1.1 – 5.1.4	Anforderungen und Prüfverfahren Neue Nummerierung aufgrund der Herausnahme der früheren Anforderungen 5.1.1 bis 5.1.3.	Erläuterung
5.1.4	5.1.1	Prüfverfahren Die Formulierung „ <i>oder werden vor der Verwendung bereinigt</i> “ wurde herausgenommen, um den wahren Zweck in den Vordergrund zu rücken.	Erläuterung
5.1.5	5.1.2	Anforderung und Prüfverfahren Es wurde verdeutlicht, dass Testdaten und -konten vor der „ <i>Freigabe an den Kunden</i> “ gelöscht werden müssen.	Erläuterung
5.1.7	5.1.4	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Die konsolidierten Testverfahren (früher 5.1.7.a und 5.1.7.b) wurden zu dem Verfahren 5.1.4.a zusammengefasst, um „interne“ und „Web“-Anwendungen in einem einzigen Verfahren zu kombinieren. Außerdem wurde das nunmehr redundante frühere Prüfverfahren 5.1.7.b entfernt. ▪ Der spezifische Verweis zu Webanwendungen und zum OWASP-Handbuch wurde herausgenommen, um die sicheren Codierungsanforderungen für alle Anwendungen, einschließlich nicht webbasierten Anwendungen, zusammenzufassen. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
5.2	5.2	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
5.2.1 – 5.2.10	5.2.1 – 5.2.9	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Die früher unter 5.2.1 bis 5.2.10 geführten Schwachstellen wurden aktualisiert und mit der früheren Anforderung 5.1.1 kombiniert, um sie dem aktuellen Handbuch des CWE, CERT und QWASP anzupassen. ▪ In den Anforderungen 5.2.7 bis 5.2.9 werden webanwendungsspezifische Schwachstellen genannt. 	Erläuterung
Nicht zutr.	5.2.6	Anforderung und Prüfverfahren Es wurde die neue Anforderung 5.2.6 eingeführt, um sich den in der Anforderung 7.1 identifizierten risikoreichen Schwachstellen zu widmen.	Neue Anforderung
5.3.2	5.3.2	Anforderungen und Prüfverfahren Die Anforderung und das Prüfverfahren wurden überarbeitet, um zu verdeutlichen, dass eine Genehmigung von autorisierten Parteien anstelle des „Managements“ erforderlich ist.	Erläuterung
5.3.3	5.3.3, 5.3.3.a – 5.3.3.b	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Der Zweck der Anforderung und des Testverfahrens 5.3.3.a für Funktionalitätstests wurde verdeutlicht, um sicherzustellen, dass die Änderungen nicht die Sicherheit des Systems beeinträchtigen. ▪ Die frühere Anforderung 5.1.1 wurde in das neue Prüfverfahren 5.3.3.b integriert, um beziehend auf 5.2 die Tests von Änderungen zu thematisieren. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
5.4	5.4	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Es wurde 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 5.4 wurde in die einzelnen Verfahren 5.4.a und 5.4.b unterteilt und es wurde eine zusätzliche Erklärung des Prüfverfahrens 5.4.b hinzugefügt, um sicherzustellen, dass alle erforderlichen Dienste bereits standardmäßig sicher konfiguriert sind. ▪ Es wurde das Prüfverfahren 5.4.c hinzugefügt, um sicherzustellen, dass das <i>PA-DSS-Implementierungshandbuch</i> alle erforderlichen Protokolle, Dienste, Daemons, Komponenten und zugehörige Software und Hardware dokumentiert. 	Erläuterung
6.1	6.1, 6.1.a – 6.1.f	Prüfverfahren <ul style="list-style-type: none"> ▪ Der Verweis zum PCI-DSS wurde entfernt und die PCI-DSS-Prüfverfahren wurden importiert, um entsprechend der Zahlungsanwendungen die neuen Prüfverfahren 6.1.a bis 6.1.f zu erstellen. ▪ Das Prüfverfahren 6.1.f wurde aktualisiert, um abzuklären, welche Anweisungen in das <i>PA-DSS-Implementierungshandbuch aufgenommen werden müssen</i>. 	Erläuterung
6.2	6.2	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Aktualisierter Hinweis bezüglich der Nutzung von WEP ab dem 30. Juni 2010. ▪ Im Prüfverfahren 6.2.b wurde der Verweis auf den PCI-DSS entfernt und es wurden bestimmte Elemente näher erläutert, die in das <i>PA-DSS-Implementierungshandbuch aufgenommen werden müssen</i>. 	Erläuterung
7.1	7.1, 7.1.a – 7.1.d	Anforderungen und Prüfverfahren <p>Die Anforderung wurde aktualisiert, um sicherzustellen, dass die erkannten Schwachstellen entsprechend dem von ihnen ausgehenden Risiko eingestuft werden. Zur Anpassung an die Anforderung wurde das zusätzliche Prüfverfahren 7.1.a aufgenommen.</p> <p>Das frühere Prüfverfahren 7.1 wurde in die einzelnen Verfahren 7.1.a bis 7.1.d unterteilt.</p>	Neue Anforderung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
7.2.a – 7.2.b	7.2.a – 7.2.e	Prüfverfahren Das frühere Prüfverfahren 7.2.a wurde in die einzelnen Verfahren 7.2.a bis 7.2.d unterteilt. Das frühere Prüfverfahren 7.2.b wurde in 7.2.e unnummeriert.	Erläuterung
10, 11	10	Anforderungen und Prüfverfahren Die Anforderungen 10 und 11 wurden zusammengefasst, um Überschneidungen zu entfernen. Die ursprüngliche Anforderung 10.1 ist nun die Anforderung 10.3.1.	Erläuterung
10, 11	10	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ Der frühere Punkt 11.1 wurde in 10.1 unnummeriert. Es wurde erklärt, dass die Zahlungsanwendung nicht mit der Nutzung von Zwei-Faktor-Authentifizierungstechnologien für einen sicheren Remote-Zugriff interferieren darf. Das Beispiel für „Radius mit Tokens“ wurde aktualisiert. ▪ Der frühere Punkt 11.2 wurde in 10.2 unnummeriert. Keine inhaltlichen Änderungen. ▪ Zum Thema Remote-Zugriff auf die Zahlungsanwendung wurde die übergeordnete Anforderung 10.3 erstellt. Die früheren Anforderungen 10.1 und 11.3 wurden jeweils in 10.3.1 und 10.3.2 unnummeriert. Keine inhaltlichen Änderungen. ▪ Die Beispiele wurden aus dem Prüfverfahren in die Anforderungsspalte verschoben. 	Erläuterung
12, 13, 14	11, 12, 13	Anforderungen und Prüfverfahren Aufgrund der Zusammenfassung der Anforderungen 10 und 11 wurden die früheren Anforderungen 12, 13 und 14 jeweils in die Anforderungen 11, 12 und 13 unnummeriert.	Erläuterung
12.1	11.1	Anforderungen und Prüfverfahren <ul style="list-style-type: none"> ▪ SSH wurde als Beispiel für ein Sicherheitsprotokoll aufgeführt und es wurden Beispiele aus den Prüfverfahren herausgenommen. ▪ Aus Konsistenzgründen wurde der Begriff „starke Kryptographie- und Sicherheitsprotokolle“ näher erklärt. 	Erläuterung

Abschnitt oder Anforderung		Änderung	Typ ⁱ
Alt	Neu		
12.2	11.2	Anforderungen Es wurde erläutert, dass diese Anforderung zutrifft, wenn die Zahlungsanwendung die Übermittlung von PANs über Messaging-Technologien für Endanwender zulässt und dass die Lösung die PAN entweder unleserlich machen oder eine starke Kryptographie implementieren muss.	Erläuterung
13.1	12.1	Anforderungen und Prüfverfahren Aus Konsistenzgründen wurde der Begriff „starke Kryptographie- und Sicherheitsprotokolle“ näher erklärt.	Erläuterung
Anhang A	Anhang A	Alle Anforderungen <ul style="list-style-type: none"> ▪ Der Inhalt des <i>PA-DSS-Implementierungshandbuchs</i> wurde aktualisiert, um die Änderungen in den PA-DSS-Anforderungen widerzuspiegeln. ▪ In Anlehnung an die PA-DSS-Anforderungen wurden die Verweise zum PCI-DSS aktualisiert. 	Erläuterung
Anhang B	Anhang B	Punkt 5.b Die Laborverfahren, die in der vorigen Version versehentlich nicht berücksichtigt wurden, wurden nun wieder eingefügt.	Erläuterung
Anhang B	Anhang B	Punkt 6.b Entsprechend der vorgenommenen Änderungen in den PA-DSS-Anforderungen 5.1 und 5.2 wurde der Verweis auf Schwachstellen aktualisiert, um sich nicht nur auf das OWASP zu stützen.	Erläuterung
Anhang B	Anhang B	Punkt 7.c Es wurde eine zusätzliche Erklärung eingefügt, dass der PA-QSA die korrekte Installation der entfernt gelegenen Laboreinrichtung bestätigen muss, um sicherzustellen, dass die Umgebung tatsächlich eine reale Situation simuliert.	Erläuterung
Anhang C	Validierungsbestätigung	Aus dem Anhang herausgenommen Das Format wurde umgestellt, um vor den PA-QSA-Informationen zunächst Informationen über Anwendungsanbieter zu liefern.	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 zusätzliche Informationen zu einem bestimmten Thema zu liefern.
Neue Anforderung	Verbesserungen	Änderungen, um sicherzustellen, dass die Standards auf dem neuesten Stand bezüglich neuer Bedrohungen und Veränderungen der Branche sind.