Payment Card Industry (PCI)
Datensicherheitsstandard

Selbstbeurteilungs-Fragebogen D
und Konformitätsbescheinigung für Händler

Alle anderen für den SBF qualifizierten Händler

Zur Verwendung mit PCI DSS Version 3.2

April 2016

Dokumentänderungen

Datum	PCI DSS Version	SBF Revision	Beschreibung
Oktober 2008	1.2		Anpassung der Inhalte an den neuen PCI DSS v1.2 und Implementieren kleinerer Änderungen nach der Ursprungsversion v1.1.
Oktober 2010	2.0		Anpassung der Inhalte an die neuen Anforderungen und Testverfahren nach PCI DSS v2.0.
Februar 2014	3.0		Anpassung der Inhalte an die Anforderungen und Testverfahren nach PCI DSS v3.0 sowie Integration weiterer Reaktionsmöglichkeiten.
April 2015	3.1		Aktualisiert im Sinne des PCI-DSS v3.1. Ausführliche Informationen finden Sie unter *PA-DSS – Änderungsübersicht von PA-DSS Version 3.0 auf 3.1*.
Juli 2015	3.1	1.1	Aktualisiert zum Entfernen von Referenzen auf “bewährte Verfahren” vor dem 30. Juni 2015 und zum Entfernen der PCI DSS v2 Berichtsoption für Anforderung 11.3.
April 2016	3.2	1.0	Aktualisiert im Sinne des PCI DSS v3.2. Ausführliche Informationen zu den Änderungen am PCI DSS finden Sie unter *PCI DSS – Änderungsübersicht von PCI DSS Version 3.1 auf 3.2*.

Inhalt

Dokumentänderungen ..... **i**

Vorbereitung ..... **iv**

PCI-DSS-Selbstbeurteilung – Schritte zum Ausfüllen ..... **iv**

Erklärungen zum Selbstbeurteilungsfragebogen ..... **iv**

Erwartete Tests ..... *v*

Ausfüllen des Selbstbeurteilungsfragebogens ..... **v**

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen ..... **vi**

Unterschied zwischen „Nicht zutreffend“ und „Nicht geprüft“ ..... *vi*

Gesetzliche Ausnahme ..... **vii**

1. Abschnitt: Informationen zur Beurteilung **1**

2. Abschnitt: Selbstbeurteilungsfragebogen D für Händler **4**

Erstellung und Wartung sicherer Netzwerke und Systeme **4**

Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten *4*

Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden *9*

Schutz von Karteninhaberdaten **16**

Anforderung 3: Schutz gespeicherter Karteninhaberdaten *16*

Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze *25*

Unterhaltung eines Anfälligkeits-Managementprogramms **27**

Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen *27*

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen *29*

Implementierung starker Zugriffskontrollmaßnahmen **40**

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf *40*

Anforderung 8: Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten *43*

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken *50*

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken **59**

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten *59*

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse *66*

Befolgung einer Informationssicherheitsrichtlinie **75**

Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal. *75*

Anhang A: Zusätzliche PCI DSS Anforderungen **83**

Anhang A1: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsamem Hosting *83*

Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden *83*

Anhang A3: Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation, DESV) *84*

Anhang B: **Arbeitsblatt – Kompensationskontrollen** **85**
Anhang C: **Erläuterung der Nichtanwendbarkeit** **86**
Anhang D: **Erklärung zu nicht geprüften Anforderungen** **87**
3. Abschnitt: **Validierungs- und Bescheinigungsdetails** **88**

Vorbereitung

SBF D für Händler richtet sich an Händler, die für den SBF qualifiziert sind und die Kriterien für andere SBF-Typen nicht erfüllen. Der SBF D findet beispielsweise in folgenden Händlerumgebungen Anwendung:

- E-Commerce-Händler, die Karteninhaberdaten auf ihrer Website akzeptieren.
- Händler mit elektronischer Speicherung von Karteninhaberdaten
- Händler, die Karteninhaberdaten nicht elektronisch speichern, jedoch nicht die Kritierien eines anderen SBF-Typs erfüllen
- Händler mit Umgebungen, die eventuell die Kriterien eines anderen SBF-Typs erfüllen, jedoch zusätzliche PCI-DSS-Anforderungen an Ihre Umgebung erfüllen müssen

Da viele Unternehmen, die SBF D ausfüllen, die Konformität mit allen PCI-DSS-Anforderungen bestätigen müssen, werden einige Unternehmen mit sehr spezifischen Geschäftsmodellen evtl. feststellen, dass einige Anforderungen für sie nicht gelten. In der nachstehenden Anleitung finden Sie Informationen über den Ausschluss spezifischer Anforderungen.

PCI-DSS-Selbstbeurteilung – Schritte zum Ausfüllen

1. Stellen Sie fest, welcher SBF für Ihre Umgebung relevant ist – Nähere Informationen finden Sie im Dokument *Anleitung und Richtlinien zum Selbstbeurteilungsfragebogen* auf der PCI-SSC-Website.
2. Bestätigen Sie, dass Ihre Umgebung dem Umfang/Geltungsbereich entspricht und die Qualifikationskriterien für den von Ihnen verwendeten SBF erfüllt.
3. Bewerten Sie Ihre Umgebung auf die Erfüllung der PCI-DSS-Anforderungen.
4. Füllen Sie alle Abschnitte des Dokuments aus:
   - 1. Abschnitt (Teil 1 und 2 der Konformitätsbescheinigung) – Informationen zur Beurteilung und Executive Summary.
   - 2. Abschnitt – PCI-DSS-Selbstbeurteilungsfragebogen (SBF D)
   - 3. Abschnitt (Teil 3 und 4 der Konformitätsbescheinigung) – Validierungs- und Bescheinigungsdetails sowie Aktionsplan für Status „Nicht konform“ (falls zutreffend)
5. Reichen Sie den SBF und die Konformitätsbescheinigung (AOC) zusammen mit allen anderen erforderlichen Dokumenten – zum Beispiel den ASV-Scan-Berichten – beim Acquirer, bei der Zahlungsmarke oder bei einer anderen Anforderungsstelle ein.

Erklärungen zum Selbstbeurteilungsfragebogen

Die Fragen in der Spalte „PCI-DSS-Frage“ in diesem Selbstbeurteilungsfragebogen basieren auf den PCI-DSS-Anforderungen.

Als Hilfe beim Beurteilungsprozess stehen weitere Ressourcen mit Hinweisen zu den PCI-DSS-Anforderungen und zum Ausfüllen des Selbsbeurteilungsfragebogens zur Verfügung. Ein Teil dieser Ressourcen ist unten aufgeführt:

Dokument	enthält:
PCI DSS *(Anforderungen und Sicherheitsbeurteilungsverfahren des PCI-Datensicherheitsstandards)*	• Leitfaden zum Umfang/Geltungsbereich • Leitfaden zum Zweck der PCI-DSS-Anforderungen • Detaillierte Informationen zu Testverfahren • Leitfaden zu Kompensationskontrollen

Dokument	enthält:
Anleitung und Richtlinien zum SBF	• Informationen zu allen SBF und ihren Qualifikationskriterien • Bestimmung des passenden SBF für Ihr Unternehmen
PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme	• Beschreibungen und Definitionen von Begriffen, die im PCI DSS und in den Selbstbeurteilungsfragebögen vorkommen

Diese und weitere Ressourcen sind auf der PCI-SSC-Website *(www.pcisecuritystandards.org)* zu finden. Unternehmen sollten vor jeder Beurteilung den PCI DSS und weitere zugehörige Dokumente durchlesen.

Erwartete Tests

Die Anweisungen in der Spalte „Expected Testing" (Erwartete Tests) basieren auf den Testverfahren im PCI DSS und beschreiben in allgemeiner Form die Testaktivitäten, mit denen die Erfüllung der Anforderungen überprüft werden sollte. Eine ausführliche Beschreibung der Testverfahren zu jeder Anforderung ist im PCI DSS zu finden.

Ausfüllen des Selbstbeurteilungsfragebogens

Zu jeder Frage gibt es mehrere Antwortmöglichkeiten. Die Antworten spiegeln den Status Ihres Unternehmens in Bezug auf die jeweilige Anforderung wider. ***Pro Frage ist nur eine Antwort auszuwählen.***

Die Bedeutung der jeweiligen Antworten ist in der Tabelle unten beschrieben:

Antwort	Wann trifft diese Antwort zu?
Ja	Die erwarteten Tests wurden durchgeführt und alle Elemente der Anforderung wurden wie angegeben erfüllt.
Ja, mit CCW (Compensating Control Worksheet, Arbeitsblatt zu Kompensationskontrollen)	Die erwarteten Tests wurden durchgeführt, und die Anforderung wurde unter Zuhilfenahme einer Kompensationskontrolle erfüllt. Für alle Antworten in dieser Spalte ist ein Arbeitsblatt zu Kompensationskontrollen (Compensating Control Worksheet, CCW) in Anhang B des SBF auszufüllen. Informationen zu Kompensationskontrollen und Hinweise zum Ausfüllen des Arbeitsblatts sind im PCI DSS enthalten.
Nein	Einige oder alle Elemente der Anforderung wurden nicht erfüllt, werden gerade implementiert oder müssen weiteren Tests unterzogen werden, ehe bekannt ist, ob sie vorhanden sind.
Nicht zutr. (Nicht zutreffend)	Die Anforderung gilt nicht für die Umgebung des Unternehmens. (Beispiele sind im *Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen* zu finden. Siehe unten.) Bei allen Antworten in dieser Spalte ist eine zusätzliche Erklärung in Anhang C des SBF erforderlich.
Nicht geprüft	Die Anforderung wurde nicht in die Beurteilung einbezogen und auch nicht anderweitig geprüft. (Beispiele für die Verwendung dieser Option finden Sie unter *Unterschied zwischen „Nicht zutreffend" und „Nicht geprüft"*.) Bei allen Antworten in dieser Spalte ist eine zusätzliche Erklärung in Anhang D des SBF erforderlich.

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

Da viele Unternehmen, die SBF D ausfüllen, die Konformität mit allen PCI-DSS-Anforderungen bestätigen müssen, werden einige Unternehmen mit sehr spezifischen Geschäftsmodellen evtl. feststellen, dass einige Anforderungen für sie nicht gelten. Ein Unternehmen, das z. B. überhaupt keine drahtlose Technologie verwendet, muss die Konformität mit den Abschnitten des PCI DSS, die sich speziell auf die Verwaltung drahtloser Technologien beziehen, nicht validieren. Ebenso muss ein Unternehmen, das zu keinem Zeitpunkt Karteninhaberdaten elektronisch speichert, die Anforderungen im Zusammenhang mit der sicheren Speicherung von Karteninhaberdaten (z. B. Anforderung 3.4) nicht validieren.

Beispiele für Anforderungen, die nur in bestimmten Fällen erfüllt werden müssen:

- Die spezifischen Fragen zur Sicherung von drahtlosen Technologien (z. B. Anforderungen 1.2.3, 2.1.1 und 4.1.1) müssen nur beantwortet werden, wenn drahtlose Technologie in Ihrem Netzwerk verwendet wird. Bitte beachten Sie, dass Anforderung 11.1 (Verwendung eines Prozesses zur Erkennung unbefugter WLAN-Zugriffspunkte) auch beantwortet werden muss, wenn Sie in Ihrem Netzwerk keine drahtlose Technologie verwenden, weil der Prozess alle sicherheitsgefährdenden oder unerlaubten Geräte erfasst, die vielleicht ohne Ihr Wissen angeschlossen wurden.
- Die spezifischen Fragen zu Anwendungsentwicklung und sicherer Codierung (Anforderungen 6.3 und 6.5) müssen nur beantwortet werden, wenn Ihr Unternehmen eigene benutzerdefinierte Anwendungen entwickelt.
- Die Fragen zu den Anforderungen 9.1.1 und 9.3 müssen nur von Stellen mit „sensiblen Bereichen“ gemäß folgender Definition beantwortet werden: „Sensible Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Dazu zählen nicht Bereiche, in denen ausschließlich Point-of-Sale-Terminals vorhanden sind, wie zum Beispiel der Kassenbereich in einem Einzelhandel. Hierin eingeschlossen sind jedoch Back-Office-Serverräume in Einzelhandelsgeschäften, in denen Karteninhaberdaten gespeichert werden, sowie Speicherbereiche für große Mengen an Karteninhaberdaten.

Gelten einzelne Anforderungen als nicht anwendbar in Ihrer Umgebung, wählen Sie für die betreffenden Anforderungen die Option „Nicht zutr.“ und füllen Sie zu jedem „Nicht zutr.“-Eintrag das Arbeitsblatt „Erklärung der Nichtanwendbarkeit“ in Anhang C aus.

Unterschied zwischen „Nicht zutreffend“ und „Nicht geprüft“

Es ist zu prüfen, ob Anforderungen in einer Umgebung als „nicht zutreffend“ klassifiziert sind. Im oben erwähnten Beispiel zu drahtlosen Technologien müsste das Unternehmen zunächst bestätigen, dass keine drahtlosen Technologien in ihrer CDE (cardholder data environment, Karteninhaberdaten-Umgebung) zum Einsatz kommen oder mit ihrer CDE verbunden sind. Erst dann kann für die Anforderungen 1.2.3, 2.1.1 und 4.1.1 „Nicht zutreffend“ ausgewählt werden. Die Bestätigung muss jedoch in jedem Fall zuvor erfolgt sein.

Wird eine Anforderung gänzlich von der Gültigkeitsprüfung *ausgeschlossen*, sollte die Option „Nicht geprüft“ ausgewählt werden. Dies kann beispielsweise in folgenden Situationen der Fall sein:

- Ein Unternehmen wird vom Acquirer gebeten, bestimmte Anforderungen zu validieren, etwa die Anwendung des bevorzugten Verfahrens zur Validierung bestimmter „Meilensteine“.
- Ein Unternehmen möchte eine neue Sicherheitskontrolle validieren, die sich nur auf bestimmte Anforderungen auswirkt, etwa die Umsetzung einer neuen Verschlüsselungsmethode, die eine Validierung der PCI-DSS-Anforderungen 2, 3 und 4 erfordert.
- Ein Dienstanbieter bietet eventuell einen Service an, der nur wenige PCI-DSS-Anforderungen umfasst. Beispiel: Ein Anbieter von physischem Speicher zieht es vor, nur die physischen Sicherheitskontrollen gemäß PCI-DSS-Anforderung 9 für seine Speichereinrichtung zu validieren.

In den beschriebenen Szenarien möchte das Unternehmen nur bestimmte PCI-DSS-Anforderungen validieren, auch wenn darüber hinaus weitere Anforderungen für ihre Umgebung gelten könnten.

Gesetzliche Ausnahme

Unterliegt Ihr Unternehmen einer gesetzlichen Beschränkung, welche die Erfüllung einer PCI-DSS-Anforderung unmöglich macht, markieren Sie für diese Anforderung die Spalte „Nein“ und füllen Sie die zugehörige Bescheinigung in Teil 3 aus.

1. Abschnitt: Informationen zur Beurteilung

Anleitung zum Einreichen

Dieses Dokument muss zur Bestätigung der Ergebnisse der Händler-Selbstbeurteilung gemäß dem *Datensicherheitsstandard der Zahlungskartenbranche (Payment Card Industry Data Security Standard, kurz PCI DSS) und den Sicherheitsbeurteilungsverfahren ausgefüllt werden.* Füllen Sie alle Abschnitte aus: Der Händler ist dafür verantwortlich, dass alle Abschnitte von den betreffenden Parteien ausgefüllt werden. Wenden Sie sich bezüglich des ordnungsgemäßen Berichts- und Einreichungsverfahrens an den Acquirer (Handelsbank) oder die Zahlungsmarken.

Teil 1. Informationen zum Qualified Security Assessor und Händler

Teil 1a. Händlerinformationen

Firma:			DBA (Geschäftstätigkeit als):		
Name des Ansprechpartners:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 1b. Informationen zur Firma des Qualified Security Assessors (falls vorhanden)

Firma:					
QSA-Leiter:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 2. Zusammenfassung für die Geschäftsleitung

Teil 2a. Handelstätigkeit (alle zutreffenden Optionen auswählen)

☐ Einzelhändler	☐ Telekommunikation	☐ Lebensmitteleinzelhandel und Supermärkte
☐ Erdöl/Erdgas	☐ E-Commerce	☐ Schriftliche/Telefonische Bestellung (MOTO)
☐ Sonstiges (bitte angeben):		

Welche Arten von Zahlungskanälen werden von Ihrem Unternehmen bedient?	Welche Zahlungskanäle sind durch diesen SBF abgedeckt?
☐ Schriftliche/Telefonische Bestellung (MOTO)	☐ Schriftliche/Telefonische Bestellung (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Vorlage der Karte (persönlich)	☐ Vorlage der Karte (persönlich)

Hinweis: *Wird einer Ihrer Zahlungskanäle oder -prozesse durch diesen SBF nicht abgedeckt, wenden Sie sich bezüglich der Validierung für die anderen Kanäle an Ihren Acquirer oder Ihre Zahlungsmarke.*

Teil 2b. Beschreibung des Zahlungskartengeschäfts

Wie und in welcher Kapazität speichert, verarbeitet bzw. überträgt Ihr Unternehmen Karteninhaberdaten?	

Teil 2c. Standorte

Führen Sie alle Einrichtungen und Standorte auf (beispielsweise Einzelhandelsgeschäfte, Büroräume, Rechenzentren, Callcenter, usw.), sowie eine Zusammenfassung der in der PCI-DSS-Prüfung enthaltenen Standorte.

Art der Einrichtung	Anzahl der Einrichtungen dieser Art	Standort(e) der Einrichtung (Ort, Land)
Beispiel: Einzelhandelsgeschäfte	*3*	*Boston, MA, USA*

Teil 2d. Zahlungsanwendung

Nutzt das Unternehmen eine oder mehrere Zahlungsanwendungen? ☐ Ja ☐ Nein

Geben Sie folgende Informationen bezüglich der Zahlungsanwendungen an, die in Ihrem Unternehmen genutzt werden:

Name der Zahlungsanwendung	Versionsnummer	Anbieter der Anwendung	Steht die Anwendung auf der PA-DSS-Liste?	Ablaufdatum der PA-DSS-Liste (falls zutreffend)
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	

Teil 2e. Beschreibung der Umgebung

Beschreiben Sie ***in allgemeiner Form*** die in dieser Beurteilung berücksichtigte Umgebung. *Beispiel:* • *Ein- und ausgehende Verbindungen zur/von der CDE (cardholder data environment, Karteninhaberdaten-Umgebung).* • *Wichtige Systemkomponenten in der CDE, etwa POS-*	

Geräte, Datenbanken und Webserver sowie weitere notwendige Zahlungskomponenten (falls zutreffend).	
Nutzt Ihr Unternehmen die Netzwerksegmentierung auf eine Weise, dass der Umfang Ihrer PCI-DSS-Umgebung davon betroffen ist? *(Hinweise zur Netzwerksegmentierung finden Sie im PCI DSS im Abschnitt „Netzwerksegmentierung“.)*	☐ Ja ☐ Nein

Teil 2f. Externe Dienstanbieter

Verwendet Ihr Unternehmen einen Qualified Integrator & Reseller (QIR)? Falls ja: Name des QIR-Unternehmens: Individuelle Bezeichnung des QIR: Beschreibung der vom QIR erbrachten Dienstleistungen:	☐ Ja ☐ Nein
Werden Karteninhaberdaten von Ihrem Unternehmen an externe Dienstanbieter (beispielsweise Gateways, Qualified Integrator & Resellers (QIR), Zahlungsabwickler, Zahlungsdienstleister (PSP), Webhosting-Unternehmen, Flugreiseagenturen, Anbieter von Kundenbindungsprogrammen) weitergegeben?	☐ Ja ☐ Nein

Falls ja:

Name des Dienstanbieters:	**Beschreibung der erbrachten Dienstleistungen:**

Hinweis: *Anforderung 12.8 gilt für alle Stellen in dieser Liste.*

2. Abschnitt: Selbstbeurteilungsfragebogen D für Händler

Hinweis: *Die folgenden Fragen wurden entsprechend den PCI-DSS-Anforderungen und Testverfahren nummeriert, so wie in den* PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren *beschrieben.*

Selbstbeurteilung abgeschlossen am:

Erstellung und Wartung sicherer Netzwerke und Systeme

Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
1.1	Wurden Standards für die Firewall- und Router-Konfiguration festgelegt und umgesetzt, die folgende Elemente beinhalten?						
1.1.1	Gibt es einen offiziellen Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration?	▪ Dokumentierten Prozess überprüfen ▪ Mitarbeiter befragen ▪ Netzwerkkonfigurationen überprüfen	☐	☐	☐	☐	☐
1.1.2	(a) Liegt ein aktuelles Netzwerkdiagramm mit allen Verbindungen zwischen der Karteninhaberdaten-Umgebung (CDE) und anderen Netzwerken, einschließlich aller drahtlosen Netzwerke, vor?	▪ Aktuelles Netzwerkdiagramm überprüfen ▪ Netzwerkkonfigurationen überprüfen	☐	☐	☐	☐	☐
	(b) Gibt es einen Prozess, mit dem die ständige Aktualität des Diagramms sichergestellt wird?	▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
1.1.3	(a) Liegt ein aktuelles Diagramm mit den system- und netzwerkübergreifenden Flüssen von Karteninhaberdaten vor?	▪ Aktuelles Datenflussdiagramm überprüfen ▪ Netzwerkkonfigurationen überprüfen	☐	☐	☐	☐	☐
	(b) Gibt es einen Prozess, mit dem die ständige Aktualität des Diagramms sichergestellt wird?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
1.1.4	(a) Ist eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone vorgeschrieben und implementiert?	▪ Standards für die Firewall-Konfiguration durchgehen ▪ Netzwerkkonfigurationen darauf überprüfen, ob eine oder mehrere Firewalls vorhanden sind	☐	☐	☐	☐	☐
	(b) Entspricht das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration?	▪ Standards der Firewall-Konfiguration mit dem aktuellen Netzwerkdiagramm vergleichen	☐	☐	☐	☐	☐
1.1.5	Sind die Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten in den Standards für die Firewall- und Router-Konfiguration zugewiesen und dokumentiert?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
1.1.6	(a) Enthalten die Konfigurationsstandards von Firewall und Router eine dokumentierte Liste von Diensten, Protokollen und Ports, einschließlich geschäftlicher Rechtfertigung und Genehmigung dieser?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen	☐	☐	☐	☐	☐
	(b) Wurden alle unsicheren Services, Protokolle und Ports identifiziert und sind die jeweiligen Sicherheitsfunktionen hierfür einzeln dokumentiert und implementiert?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen ▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.1.7	(a) Erfordern die Standards für die Firewall- und Router-Konfiguration mindestens alle sechs Monate eine Prüfung von Firewall- und Router-Regeln?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen	☐	☐	☐	☐	☐
	(b) Werden die Firewall- und Router-Regeln mindestens alle sechs Monate überprüft?	▪ Dokumentation der Firewall-Überprüfungen durchgehen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
1.2	Schränken die Firewall- und Router-Konfigurationen die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und sämtlichen Systemen in der Karteninhaberdaten-Umgebung wie folgt ein? ***Hinweis:*** *Ein „nicht vertrauenswürdiges Netzwerk" ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.*							
1.2.1	(a) Ist der ein- und ausgehende Netzwerkverkehr auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Verkehr beschränkt?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen ▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
	(b) Wird der restliche ein- und ausgehende Verkehr eigens abgelehnt (z. B. durch die Verwendung einer ausdrücklichen „Alle ablehnen"-Anweisung oder einer impliziten Anweisung zum Ablehnen nach dem Zulassen)?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen ▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.2.2	Sind die Router-Konfigurationsdateien vor unbefugtem Zugriff gesichert und synchronisiert – stimmt beispielsweise die ausgeführte (oder aktive) Konfiguration mit der Startkonfiguration (für das Hochfahren von Computern) überein?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen ▪ Router-Konfigurationsdateien und Router-Konfigurationen überprüfen	☐	☐	☐	☐	☐
1.2.3	Sind Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der CDE und Konfigurieren dieser Firewalls installiert und so konfiguriert, dass der gesamte Verkehr zwischen der drahtlosen Umgebung und der CDE abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt?	▪ Standards für die Firewall- und Router-Konfiguration durchgehen ▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
1.3	Verbietet die Firewall-Konfiguration wie folgt den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung?						
1.3.1	Ist eine DMZ implementiert, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich zugängliche Dienste, Protokolle und Ports anbieten.	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.3.2	Ist der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt?	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.3.3	Sind Anti-Spoofing-Maßnahmen zur Erkennung und Blockierung gefälschter Quell-IP-Adressen, über die auf das Netzwerk zugegriffen wird, implementiert? (So kann beispielsweise der Datenverkehr blockiert werden, der trotz einer internen Adresse über das Internet zuzugreifen versucht.)	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.3.4	Ist die Weiterleitung ausgehenden Datenverkehrs von der Karteninhaberdaten-Umgebung an das Internet ausdrücklich erlaubt?	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.3.5	Sind nur etablierte Verbindungen in das Netzwerk zulässig?	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
1.3.6	Sind Systemkomponenten, die Karteninhaberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone gespeichert, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist?	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
1.3.7	(a) Wurden Methoden implementiert, um die Offenlegung privater IP-Adressen und Routing-Informationen an das Internet zu verhindern? ***Hinweis:*** *Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderem:* • Network Address Translation (NAT); • das Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls; • Löschen oder Filtern von Route-Advertisements für private Netzwerke, die registrierte Adressen verwenden; • Interne Nutzung eines RFC1918-Adressraums anstatt registrierter Adressen.	▪ Firewall- und Router-Konfigurationen untersuchen	☐	☐	☐	☐	☐
	(b) Dürfen private IP-Adressen und Routing-Informationen an externe Stellen weitergegeben werden?	▪ Firewall- und Router-Konfigurationen untersuchen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
1.4	(a) Ist eine persönliche Firewall-Software auf allen mobilen und/oder den Mitarbeitern gehörenden Geräten installiert, die außerhalb des Netzwerks auf das Internet zugreifen (z. B. Laptops, die von Mitarbeitern verwendet werden) und die auch für den Zugriff auf das Netzwerk eingesetzt werden?	▪ Richtlinien und Konfigurationsstandards überprüfen ▪ Mobile und/oder mitarbeitereigene Geräte untersuchen	☐	☐	☐	☐	☐
	(b) Ist die persönliche Firewall-Software gemäß spezifischen Konfigurationseinstellungen konfiguriert, wird sie aktiv ausgeführt und ist sie nicht durch Benutzer mobiler und/oder mitarbeitereigener Geräte veränderbar?	▪ Richtlinien und Konfigurationsstandards überprüfen ▪ Mobile und/oder mitarbeitereigene Geräte untersuchen	☐	☐	☐	☐	☐
1.5	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung der Firewalls …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
2.1	(a) Werden vom Anbieter gelieferte Standardeinstellungen immer geändert, bevor ein System im Netzwerk installiert wird? *Dies gilt für SÄMTLICHE Standardkennwörter, wie etwa die von Betriebssystemen, Sicherheitssoftware, Anwendungs-und Systemkonten, POS (Point of Sale, Verkaufsstelle)-Terminals, Zahlungsanwendungeb, SNMP (Simple Network Management Protocol)-Community-Zeichenfolgen usw.).*	▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation überprüfen ▪ Systemkonfigurationen und Kontoeinstellungen prüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Werden unnötige Standardkonten vor der Installation eines Systems im Netzwerk entfernt oder deaktiviert?	▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen und Kontoeinstellungen untersuchen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
2.1.1	Für drahtlose Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder die Karteninhaberdaten übertragen, werden ALLE Standardeinstellungen des Wireless-Anbieters wie folgt geändert?						
	(a) Werden Standardwerte der Verschlüsselungsschlüssel zum Zeitpunkt der Installation geändert und werden sie jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt?	▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Werden Standard-SNMP-Community-Zeichenfolgen	▪ Richtlinien und Verfahren	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	auf drahtlosen Geräten bei der Installation geändert?	durchgehen ▪ Anbieterdokumentation durchgehen ▪ Mitarbeiter befragen ▪ Systemkonfigurationen untersuchen					
	(c) Werden Standardkennwörter/-sätze auf Zugriffspunkten bei der Installation geändert?	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
	(d) Wird die Firmware auf drahtlosen Geräten aktualisiert, um eine starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen?	▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
	(e) Werden gegebenenfalls auch andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen geändert?	▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
2.2	(a) Werden für alle Systemkomponenten Konfigurationsstandards entwickelt und sind diese mit den branchenüblichen Systemhärtungsstandards vereinbar? *Zu den Quellen für branchenübliche Systemhärtungsstandards gehören u. a. SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) und Center for Internet Security (CIS).*	▪ Standards für die Systemkonfiguration durchgehen ▪ Branchenübliche Härtungsstandards durchgehen ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Werden die Systemkonfigurationsstandards gemäß Anforderung 6.1 aktualisiert, sobald neue Schwachstellen identifiziert werden?	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(c) Werden neue Systemkonfigurationsstandards angewendet, sobald neue Systeme konfiguriert werden?	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(d) Umfassen die festgelegten Konfigurationsstandards alle nachfolgenden Punkte? • Ändern sämtlicher Standards der Anbieter und Löschen unnötiger Standardkonten • Implementieren von nur einer primären Funktion pro Server, um zu vermeiden, dass auf einem Server Funktionen mit verschiedenen Sicherheitsniveauanforderungen vorhanden sind • Aktivieren der Dienste, Protokolle, Daemons usw., die für die Systemfunktion unbedingt erforderlich sind • Implementieren zusätzlicher Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden • Konfigurieren von Systemsicherheitsparametern zur Missbrauchsvermeidung • Entfernen aller unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver	▪ Standards für die Systemkonfiguration durchgehen	☐	☐	☐	☐	☐
2.2.1	(a) Ist nur eine primäre Funktion pro Server implementiert, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveauanforderungen existieren? *Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.*	▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
	(b) Wenn Virtualisierungstechnologien eingesetzt werden, ist pro virtuelle Systemkomponente oder Gerät nur eine primäre Funktion implementiert?	▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
2.2.2	(a) Werden für den Betrieb des Systems nur notwendige Dienste, Protokolle, Daemons usw. aktiviert (d. h. nicht direkt für die Ausführung der spezifischen Gerätefunktion erforderliche Funktionen werden deaktiviert)?	▪ Konfigurationsstandards durchgehen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
	(b) Sind alle aktivierten unsicheren Dienste, Daemons oder Protokolle durch die dokumentierten Konfigurationsstandards legitimiert?	▪ Konfigurationsstandards durchgehen ▪ Mitarbeiter befragen ▪ Konfigurationseinstellungen untersuchen ▪ Aktivierte Dienste usw. mit den dokumentierten Rechtfertigungen vergleichen	☐	☐	☐	☐	☐
2.2.3	Sind zusätzliche Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden, dokumentiert und implementiert? ***Hinweis:*** *Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 abgeschlossen werden.*	▪ Konfigurationsstandards durchgehen ▪ Konfigurationseinstellungen untersuchen ▪	☐	☐	☐	☐	☐
2.2.4	(a) Verstehen sich Systemadministratoren und/oder Mitarbeiter, die Systemkomponenten konfigurieren, auf allgemeine Sicherheitsparametereinstellungen für diese Systemkomponenten?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Sind in den Systemkonfigurationsstandards gängige Sicherheitsparametereinstellungen enthalten?	▪ Standards für die Systemkonfiguration durchgehen	☐	☐	☐	☐	☐
	(c) Sind die Sicherheitsparametereinstellungen auf den Systemkomponenten sachgemäß eingestellt?	▪ Systemkomponenten untersuchen ▪ Sicherheitsparametereinstellungen untersuchen ▪ Einstellungen mit Systemkonfigurationsstandards vergleichen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
2.2.5	(a) Wurden alle unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver entfernt?	▪ Sicherheitsparameter auf Systemkomponenten untersuchen	☐	☐	☐	☐	☐
	(b) Werden aktivierte Funktionen dokumentiert und sind sie sicher konfiguriert?	▪ Dokumentation durchgehen ▪ Sicherheitsparameter auf Systemkomponenten untersuchen	☐	☐	☐	☐	☐
	(c) Sind auf den Systemkomponenten ausschließlich dokumentierte Funktionen vorhanden?	▪ Dokumentation durchgehen ▪ Sicherheitsparameter auf Systemkomponenten untersuchen	☐	☐	☐	☐	☐
2.3	Ist der Nichtkonsolen-Verwaltungszugriff wie folgt verschlüsselt? ***Hinweis*:** *Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 abgeschlossen werden*						
	(a) Werden alle Nichtkonsolen-Verwaltungszugriffe mit einer starken Kryptographie verschlüsselt und wird eine starke Verschlüsselungsmethode aufgerufen, bevor das Administratorkennwort angefordert wird?	▪ Systemkomponenten untersuchen ▪ Systemkonfigurationen untersuchen ▪ Administratoranmeldung überprüfen	☐	☐	☐	☐	☐
	(b) Sind die Systemdienste und -parameterdateien so konfiguriert, dass die Nutzung von Telnet und anderen unsicheren Remote-Anmeldebefehlen verhindert wird?	▪ Systemkomponenten untersuchen ▪ Dienste und Dateien untersuchen	☐	☐	☐	☐	☐
	(c) Ist der Administratorzugriff auf die webbasierten Managementschnittstellen mit einer starken Kryptographie verschlüsselt?	▪ Systemkomponenten untersuchen ▪ Administratoranmeldung überprüfen	☐	☐	☐	☐	☐
	(d) Wird für die eingesetzte Technologie eine starke Kryptographie gemäß den bewährten Branchenverfahren und/oder Anbieterempfehlungen implementiert?	▪ Systemkomponenten untersuchen ▪ Anbieterdokumentation durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	▪	▪					
	▪	▪					
2.4	(a) Wird ein Inventar für Systemkomponenten, die im Geltungsbereich der PCI DSS enthalten sind, geführt – einschließlich einer Liste der Hardware- und Softwarekomponenten sowie einer Funktions-/Anwendungsbeschreibung jeder einzelnen Komponente?	▪ Systeminventar überprüfen	☐	☐	☐	☐	☐
	(b) Wird das dokumentierte Inventar auf dem neuesten Stand gehalten?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
2.5	Sind Sicherheitsrichtlinien und betriebliche Verfahren zum Management der Anbieterstandardeinstellungen oder anderer Sicherheitsparameter …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
2.6	*Diese Anforderung gilt nur für Dienstanbieter.*						

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.1	Umfassen die Richtlinien, Verfahren und Prozesse zur Datenaufbewahrung und zum Löschen von Daten folgende Punkte?						
	(a) Sind die Speichermenge und die Aufbewahrungszeit der Daten auf die für rechtliche, gesetzliche und/oder geschäftliche Zwecke festgelegten Vorgaben begrenzt?	▪ Richtlinien und Verfahren zum Aufbewahren und Löschen von Daten überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Wurden Prozesse für das sichere Löschen von Karteninhaberdaten festgelegt, wenn diese Daten nicht mehr für rechtliche, gesetzliche und/oder geschäftliche Zwecke benötigt werden?	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Verfahren zum Löschen von Daten untersuchen	☐	☐	☐	☐	☐
	(c) Gelten spezifische Anforderungen für die Aufbewahrung von Karteninhaberdaten? *Karteninhaberdaten müssen z. B. für den Zeitraum X aus den Geschäftsgründen Y aufbewahrt werden.*	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Aufbewahrungsanforderungen untersuchen	☐	☐	☐	☐	☐
	(d) Wurde ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten eingeführt, die den festgelegten Aufbewahrungszeitraum überschritten haben	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Löschprozesse verfolgen	☐	☐	☐	☐	☐
	(e) Erfüllen alle gespeicherten Karteninhaberdaten die in der Datenaufbewahrungsrichtlinie beschriebenen Anforderungen?	▪ Dateien und Systemdatensätze überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.2	(a) *Dieses Testverfahren gilt nur für Kartenemittenten.*						
	(b) *Dieses Testverfahren gilt nur für Kartenemittenten.*						
	(c) Werden vertrauliche Authentifizierungsdaten nach Abschluss des Autorisierungsprozesses so gelöscht, dass sie nicht wiederhergestellt werden können?	▪ Richtlinien und Verfahren durchgehen ▪ Systemkonfigurationen untersuchen ▪ Löschprozesse untersuchen	☐	☐	☐	☐	☐
	(d) Halten alle Systeme die folgenden Anforderungen hinsichtlich des Verbots, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern, ein (auch wenn diese verschlüsselt sind)?						
3.2.1	Wird der gesamte Inhalt einer Spur auf dem Magnetstreifen (auf der Rückseite einer Karte, gleichwertige Daten auf einem Chip oder an einer anderen Stelle) nach der Autorisierung nicht gespeichert? *Diese Daten werden auch als Spurdaten, Full-Track-Daten, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet.* ***Hinweis:** Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:* • *Der Name des Karteninhabers,* • *Primäre Kontonummer (PAN),* • *Ablaufdatum und* • *Servicecode* *Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.*	▪ Datenquellen untersuchen, insbesondere: • Eingehende Transaktionsdaten • Sämtliche Protokolle • Verlaufsdateien • Trace-Dateien • Datenbankschema • Datenbankinhalte	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.2.2	Wird der Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte) nach der Autorisierung tatsächlich nicht gespeichert?	▪ Datenquellen untersuchen, insbesondere: • Eingehende Transaktionsdaten • Sämtliche Protokolle • Verlaufsdateien • Trace-Dateien • Datenbankschema • Datenbankinhalte	☐	☐	☐	☐	☐
3.2.3	Wird die persönliche Identifizierungsnummer (PIN) oder der verschlüsselte PIN-Block nach der Autorisierung nicht gespeichert?	▪ Datenquellen untersuchen, insbesondere: • Eingehende Transaktionsdaten • Sämtliche Protokolle • Verlaufsdateien • Trace-Dateien • Datenbankschema • Datenbankinhalte	☐	☐	☐	☐	☐
3.3	Wird die PAN zum Teil verborgen (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), sodass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können? ***Hinweis:*** *Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. bei juristischen Anforderungen und Anforderungen der Kreditkartenunternehmen an POS-Belege.*	▪ Richtlinien und Verfahren durchgehen ▪ Die Rollen überprüfen, welche die vollständige PAN einsehen müssen. ▪ Systemkonfigurationen untersuchen ▪ PAN-Anzeigen beobachten	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.4	Wird die PAN mithilfe eines der folgenden Verfahren überall dort unleserlich gemacht, wo sie gespeichert wird (auch auf Daten-Repositories, tragbaren digitalen Medien, Sicherungsmedien und in Prüfprotokollen)? ▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden); ▪ Abkürzung (Hashing kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen); ▪ Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden); ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren. ***Hinweis:*** *Für eine Person mit böswilligen Absichten ist es eine relativ einfache Übung, die originalen PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die abgekürzte als auch auf die Hash-Version einer PAN hat. Wenn die gehashte und die abgekürzte Version derselben PAN in der Umgebung derselben Stelle nebeneinander bestehen, müssen zusätzliche Kontrollen eingesetzt werden, damit die originale PAN nicht durch den Vergleich von gehashten und abgekürzten Versionen rekonstruiert werden kann.*	▪ Anbieterdokumentation überprüfen ▪ Daten-Repositorys untersuchen ▪ Austauschbare Datenträger untersuchen ▪ Prüfprotokolle, einschließlich Protokolle von Zahlungsanwendungen untersuchen	☐	☐	☐	☐	☐
3.4.1	Falls Festplattenverschlüsselung (statt Datenbankverschlüsselung auf Datei- oder Spaltenebene) verwendet wird: ***Hinweis:*** *Diese Anforderung gilt zusätzlich zu allen anderen PCI-DSS-Anforderungen und Schlüsselverwaltungsanforderungen.*						

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(a) Wird der logische Zugriff auf verschlüsselte Dateisysteme getrennt und unabhängig von nativen Authentifizierungs- und Zugriffskontrollmechanismen des Betriebssystems verwaltet (z. B. indem keine lokalen Benutzerkontodatenbanken oder allgemeinen Netzwerkanmeldedaten verwendet werden)?	▪ Systemkonfigurationen untersuchen ▪ Authentifizierungsprozesse überprüfen	☐	☐	☐	☐	☐
	(b) Werden kryptographische Schlüssel sicher gespeichert (z. B. auf austauschbaren Datenträgern, die durch starke Zugriffskontrollen entsprechend geschützt sind)?	▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(c) Werden Karteninhaberdaten auf austauschbaren Datenträgern unabhängig vom Speicherort verschlüsselt? ***Hinweis:*** *Wenn keine Festplattenverschlüsselung zur Verschlüsselung von Wechseldatenträgern eingesetzt wird, müssen die auf diesen Datenträgern gespeicherten Daten mithilfe einer anderen Methode unlesbar gemacht werden.*	▪ Systemkonfigurationen untersuchen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
3.5	Werden wie folgt Schlüssel verwendet, um die Karteninhaberdaten vor Weitergabe und Missbrauch zu schützen? ***Hinweis:*** *Diese Anforderung gilt für Schlüssel, die zum Verschlüsseln gespeicherter Karteninhaberdaten verwendet werden, und für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von Schlüsseln zum Verschlüsseln von Daten verwendet werden. Diese Schlüssel zum Verschlüsseln von Schlüsseln müssen mindestens so sicher wie der Schlüssel zum Verschlüsseln von Daten sein.*							
3.5.1	*Diese Anforderung gilt nur für Dienstanbieter*						
3.5.2	Ist der Zugriff auf kryptographische Schlüssel auf die geringstmögliche Anzahl von Wächtern beschränkt?	▪ Benutzerzugriffslisten überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.5.3	Werden geheime und private Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten in einer (oder mehreren) der folgenden Formen gespeichert? ▪ Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel, der mindestens so sicher wie der Datenverschlüsselungsschlüssel ist und separat von diesem gespeichert wird ▪ Speicherung in einem sicheren kryptographischen System (wie einem HSM (Host Security Module, Host-Sicherheitsmodul) oder einem für PTS zugelassenen POI-Gerät (Point Of Interaction, Interaktionspunkt) ▪ Speicherung gemäß branchenweit akzeptierter Methoden in mindestens zwei Schlüsselkomponenten voller Länge oder in Schlüssel-Shares. ***Hinweis:*** *Öffentliche Schlüssel müssen nicht in dieser Form gespeichert werden.*	▪ Dokumentierte Verfahren überprüfen ▪ Systemkonfigurationen und Schlüsselspeicherorte, einschließlich der Speicherorte von Schlüsselverschlüsselungsschlüsseln, untersuchen	☐	☐	☐	☐	☐
3.5.4	Werden kryptographische Schlüssel sicher an möglichst wenigen Speicherorten gespeichert?	▪ Schlüsselspeicherorte untersuchen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
3.6	(a) Werden alle Schlüsselverwaltungsprozesse und -verfahren für die zur Verschlüsselung von Karteninhaberdaten verwendeten kryptographischen Schlüssel vollständig dokumentiert und implementiert?	▪ Schlüsselverwaltungsverfahren untersuchen	☐	☐	☐	☐	☐
	(b) *Dieses Testverfahren gilt nur für Dienstanbieter.*						
	(c) Umfassen die implementierten Schlüsselverwaltungsprozesse und -verfahren folgende Punkte?						

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.6.1	Umfassen die Verfahren für kryptographische Schlüssel die Generierung starker kryptographischer Schlüssel?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Methode zur Schlüsselgenerierung überprüfen	☐	☐	☐	☐	☐
3.6.2	Umfassen die Verfahren für kryptographische Schlüssel die Verteilung sicherer kryptographischer Schlüssel?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Schlüsselverteilungsverfahren beobachten	☐	☐	☐	☐	☐
3.6.3	Umfassen die Verfahren für kryptographische Schlüssel die sichere Speicherung kryptographischer Schlüssel?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Methode zur sicheren Speicherung von Schlüsseln überprüfen	☐	☐	☐	☐	☐
3.6.4	Umfassen die Verfahren für kryptographische Schlüssel Änderungen kryptographischer Schlüssel für Schlüssel, die das Ende ihrer Schlüssellebensdauer erreicht haben (z. B. nach Ablauf einer festgelegten Zeitspanne und/oder nachdem von einem bestimmten Schlüssel eine gegebene Menge an Geheimtext generiert wurde), so wie von dem entsprechenden Anwendungsanbieter oder Schlüsselinhaber definiert und von bewährten Branchenverfahren und -richtlinien vorgegeben (z. B. NIST Special Publication 800-57)?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.6.5	(a) Umfassen die Verfahren für kryptographische Schlüssel die Entfernung oder den Austausch kryptographischer Schlüssel (z. B. mittels Archivierung, Vernichtung und/oder Rückruf), wenn die Integrität des Schlüssels gefährdet ist (z. B. nach Ausscheiden eines Mitarbeiters, der einen Klartext-Schlüssel kennt)?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Umfassen die Verfahren für kryptographische Schlüssel den Austausch von Schlüsseln, bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(c) Wenn entfernte oder ausgetauschte kryptographische Schlüssel aufbewahrt werden, werden diese Schlüssel ausschließlich für Entschlüsselungs-/Überprüfungszwecke und nicht zur Verschlüsselung verwendet?	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
3.6.6	Wird bei einer manuellen Verwaltung kryptographischer Klartext-Schlüssel das Prinzip der geteilten Kenntnis und doppelten Kontrollen wie folgt umgesetzt? ▪ Sehen die Verfahren, mit denen das Prinzip der geteilten Kenntnis umgesetzt wird, vor, dass sich die Schlüsselkomponenten sich in der Kontrolle von mindestens zwei Personen befinden, die jeweils nur Kenntnis über ihre eigenen Komponenten haben? UND ▪ Sehen die Verfahren zur doppelten Kontrolle vor, dass das Schlüsselmanagement von mindestens zwei Personen durchgeführt werden muss, wobei diese Personen nicht auf die Authentifizierungsdaten des jeweils anderen (z. B. Kennwörter oder Schlüssel) zugreifen können? ***Hinweis:*** *Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen: Schlüsselgenerierung, Übertragung, Ladung, Speicherung und Vernichtung.*	▪ Schlüsselverwaltungsverfahren untersuchen ▪ Mitarbeiter befragen und/oder ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
3.6.7	Umfassen die Verfahren für kryptographische Schlüssel Verfahren zur Prävention nicht autorisierter Ersetzungen kryptographischer Schlüssel?	▪ Verfahren überprüfen ▪ Mitarbeiter befragen und/oder ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
3.6.8	Müssen Wächter kryptographischer Schlüssel formal bestätigen (entweder schriftlich oder elektronisch), dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen?	▪ Verfahren überprüfen ▪ Dokumentation oder sonstige Nachweise überprüfen	☐	☐	☐	☐	☐
3.7	Sind Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
4.1	(a) Werden eine starke Kryptographie und Sicherheitsprotokolle eingesetzt, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen? ***Hinweis:*** *Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 abgeschlossen werden.* *Zu den offenen, öffentlichen Netzwerken gehören insbesondere das Internet, Drahtlostechnologien wie 802.11 und Bluetooth sowie Mobilfunktechnologien wie Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) und General Packet Radio Service (GPRS).*	▪ Dokumentierte Standards durchgehen ▪ Richtlinien und Verfahren durchgehen ▪ Alle Standorte, an denen CHD übertragen oder empfangen wird, überprüfen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
	(b) Werden ausschließlich vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert?	▪ Eingehende und ausgehende Übertragungen überprüfen ▪ Schlüssel und Zertifikate untersuchen	☐	☐	☐	☐	☐
	(c) Sind Sicherheitsprotokolle implementiert, um ausschließlich sichere Konfigurationen zu verwenden und keine unsicheren Versionen oder Konfigurationen zu unterstützen?	▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
	(d) Wird für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet (siehe Anbieterempfehlungen/bewährte Verfahren)?	▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(e) Wird bei TLS-Implementierungen bei jeder Übertragung bzw. bei jedem Empfang von Karteninhaberdaten TLS aktiviert? *Bei browserbasierten Implementierungen ist beispielsweise Folgendes zu prüfen:* • *Wird „HTTPS“ als Bestandteil des Browser-URL-Protokolls angezeigt?* • Werden Karteninhaberdaten nur angefordert, wenn die URL die Komponente „HTTPS“ enthält?	▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
		▪					
	▪	▪					
4.1.1	Werden bewährte Branchenverfahren eingesetzt, um eine starke Verschlüsselung in der Authentifizierung und Übertragung für drahtlose Netzwerke zu implementieren, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind?	▪ Dokumentierte Standards durchgehen ▪ Drahtlose Netzwerke überprüfen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
4.2	(a) Werden PANs unleserlich gemacht oder mit einer starken Kryptographie gesichert, wenn sie über Messaging-Technologien für Endanwender gesendet werden (z. B. per E-Mail, Instant Messaging, Chat, etc.)?	▪ Prozesse überprüfen ▪ Ausgehende Übertragungen überprüfen	☐	☐	☐	☐	☐
	(b) Sind Richtlinien vorhanden, die festlegen, dass ungeschützte PANs nicht über Messaging-Technologien für Endanwender gesendet werden dürfen?	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
4.3	Sind Sicherheitsrichtlinien und betriebliche Verfahren zum Verschlüsseln der Übertragung von Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Unterhaltung eines Anfälligkeits-Managementprogramms

Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
5.1	Ist eine Antivirensoftware auf allen Systemen, die üblicherweise das Ziel böswilliger Software sind, implementiert?	▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
5.1.1	Sind die Virenschutzprogramme in der Lage, bekannte Malware-Typen (z. B. Viren, Trojaner, Würmer, Spyware, Adware und Rootkits) zu erkennen, zu entfernen und vor ihnen zu schützen?	▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
5.1.2	Wird bei Systemen, die in der Regel nicht von Malware befallen sind, regelmäßig geprüft, ob sich die Malware-Bedrohung erhöht hat und diese Systeme unverändert weiter genutzt werden können?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
5.2	Es ist zu überprüfen, ob bei allen Antivirenmechanismen Folgendes beachtet wird:						
	(a) Sind die Antivirensoftware und die Definitionen immer auf dem neuesten Stand?	▪ Richtlinien und Verfahren untersuchen ▪ Antiviren-Konfigurationen einschließlich der Master-Installation untersuchen ▪ Systemkomponenten untersuchen	☐	☐	☐	☐	☐
	(b) Sind automatische Updates und regelmäßige Scans aktiviert und werden sie regelmäßig durchgeführt?	▪ Antiviren-Konfigurationen einschließlich der Master-Installation untersuchen ▪ Systemkomponenten untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(c) Generieren alle Virenschutzmechanismen Prüfprotokolle und werden die Protokolle gemäß PCI-DSS-Anforderung 10.7 aufbewahrt?	▪ Antiviren-Konfigurationen untersuchen ▪ Prozesse zur Aufbewahrung von Protokollen durchgehen	☐	☐	☐	☐	☐
5.3	Aspekte bei Antivirenmechanismen: ▪ Werden alle Antivirenmechanismen aktiv ausgeführt? ▪ Sind sie gegen benutzerseitige Deaktivierungen oder Veränderungen gesichert? ***Hinweis:*** *Antivirenlösungen können nur dann vorübergehend deaktiviert werden, wenn es einen triftigen technischen Grund dafür gibt. Dieser muss vom Management fallweise autorisiert werden. Wenn der Virenschutz aus bestimmten Gründen deaktiviert werden muss, ist hierfür eine förmliche Autorisierung erforderlich. Zusätzliche Sicherheitsmaßnahmen müssen auch für den Zeitraum, in dem der Virenschutz nicht aktiv ist, getroffen werden.*	▪ Antiviren-Konfigurationen untersuchen ▪ Systemkomponenten untersuchen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
5.4	Sind Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz von Systemen gegen Malware …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.1	Gibt es einen Prozess zur Erkennung folgender und anderer Sicherheitsrisiken? ▪ Nutzung verlässlicher externer Informationsquellen ▪ Zuweisung von Risikostufen für Sicherheitsrisiken mit der Ermittlung sämtlicher „hohen“ und „kritischen“ Risiken ***Hinweis**: Die Risikostufen sollten auf den bewährten Verfahren der Branche beruhen und die potenziellen Auswirkungen berücksichtigen. So könnten der CVSS-Basiswert und/oder die Klassifizierung durch den Anbieter sowie die Art der betroffenen Systeme als Kriterien für die Einteilung der Sicherheitsrisiken in verschiedene Stufen dienen.* *Die Methoden zur Bewertung der Sicherheitsrisiken und zur Einteilung in Sicherheitsstufen hängen von der Unternehmensumgebung und der Strategie zur Risikobewertung ab. Bei der Risikoeinstufung müssen zumindest die Sicherheitsrisiken ermittelt werden, die als „hohes Risiko“ für die Umgebung gelten. Zusätzlich zu der Risikoeinstufung können einzelne Sicherheitsrisiken als „kritisch“ betrachtet werden, falls sie eine unmittelbare Bedrohung der Umgebung darstellen, sich auf wichtige Systeme auswirken und/oder eine potenzielle Gefährdung darstellen, wenn nicht auf sie eingegangen wird. Beispiele für wichtige Systeme sind Sicherheitssysteme, öffentlich zugängliche Geräte und Systeme, Datenbanken und andere Systeme, in denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden.*	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.2	(a) Sind alle Systemkomponenten und Softwareanwendungen mithilfe der neuesten Sicherheitspatches des jeweiligen Anbieters vor bekannten Sicherheitsrisiken geschützt?	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
	(b) Werden wichtige Sicherheitspatches innerhalb eines Monats nach der Freigabe installiert? ***Hinweis**: Kritische Sicherheitspatches müssen gemäß dem in Anforderung 6.1 festgelegten Prozess zur Risikoeinstufung ermittelt werden.*	▪ Richtlinien und Verfahren durchgehen ▪ Systemkomponenten untersuchen ▪ Liste der installierten Sicherheitspatches mit der Liste der neuesten Anbieterpatches vergleichen	☐	☐	☐	☐	☐
6.3	(a) Basieren die Softwareentwicklungsprozesse auf Branchenstandards und/oder Best Practices?	▪ Softwareentwicklungsprozesse überprüfen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Ist die Informationssicherheit durchweg über den gesamten Softwareentwicklungszyklus integriert?	▪ Softwareentwicklungsprozesse überprüfen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(c) Werden Softwareanwendungen gemäß dem PCI-DSS entwickelt (z. B. sichere Authentifizierung und Protokollierung)?	▪ Softwareentwicklungsprozesse überprüfen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(d) Gewährleisten die Softwareentwicklungsprozesse folgende Punkte unter 6.3.1 bis 6.3.2?						
6.3.1	Werden Konten, Benutzer-IDs und Kennwörter für Entwicklung, Tests und/oder individuelle Anwendungen entfernt, bevor die Anwendungen aktiv oder für Kunden freigegeben werden?	▪ Softwareentwicklungsprozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.3.2	Werden alle benutzerdefinierten Codes vor der Freigabe an die Produktion oder an Kunden überprüft (entweder mithilfe manueller oder automatischer Prozesse), um alle potenziellen Sicherheitsrisiken bei der Programmierung wie folgt zu identifizieren? ▪ Werden Codeänderungen von anderen Personen als dem ursprünglichen Ersteller des Codes sowie von Personen geprüft, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind? ▪ Wird mit Codeprüfungen dafür gesorgt, dass der Code gemäß Richtlinien zur sicheren Codierung erstellt wird? ▪ Werden vor der Freigabe entsprechende Korrekturen implementiert? ▪ Werden die Ergebnisse der Codeprüfung vor der Freigabe vom Management geprüft und genehmigt? ***Hinweis**: Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus. Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. Für die Öffentlichkeit bestimmte Webanwendungen unterliegen auch zusätzlichen Kontrollen, um laufende Bedrohungen und Sicherheitsrisiken nach der Implementierung gemäß der Definition in PCI DSS-Anforderung 6.6 anzugehen.*	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Neueste Änderungen und Änderungsdokumentation überprüfen	☐	☐	☐	☐	☐
6.4	Werden Änderungskontrollprozesse und -verfahren für alle Änderungen an Systemkomponenten befolgt, um die nachstehenden Aspekte abzudecken?						
6.4.1	(a) Sind Entwicklungs-/Testumgebungen von der Produktionsumgebung getrennt?	▪ Prozesse und Verfahren zur Änderungskontrolle überprüfen ▪ Netzwerkdokumentation und Konfiguration von Netzwerkgeräten untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(b) Wurde eine Zugriffskontrolle eingeführt, um die Trennung zwischen Entwicklungs-/Testumgebungen und der Produktionsumgebung zu bewirken?	▪ Prozesse und Verfahren zur Änderungskontrolle überprüfen ▪ Zugriffskontrolleinstellungen überprüfen	☐	☐	☐	☐	☐
6.4.2	Gibt es zwischen den Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und den Mitarbeitern, die der Produktionsumgebung zugeteilt sind, eine Aufgabentrennung?	▪ Prozesse und Verfahren zur Änderungskontrolle überprüfen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
6.4.3	Werden Produktionsdaten (Live-PANs) tatsächlich ***nicht*** zum Testen oder in der Entwicklung verwendet?	▪ Prozesse und Verfahren zur Änderungskontrolle überprüfen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen ▪ Testdaten untersuchen	☐	☐	☐	☐	☐
6.4.4	Werden Testdaten und -konten aus Systemkomponenten entfernt, bevor das System aktiv wird / in Produktion geht?	▪ Prozesse und Verfahren zur Änderungskontrolle überprüfen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen ▪ Produktionssysteme untersuchen	☐	☐	☐	☐	☐
6.4.5	(a) Werden Verfahren der Änderungskontrolle dokumentiert und erfordern diese Folgendes? • Dokumentation der Auswirkungen • Dokumentierte Genehmigung der Änderungskontrolle durch autorisierte Parteien • Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt. • Back-Out-Verfahren	▪ Prozesse und Verfahren zur Änderungskontrolle überprüfen	☐	☐	☐	☐	☐
	(b) Werden die folgenden Aktivitäten bei allen Änderungen durchgeführt und dokumentiert?						

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.4.5.1	Dokumentation der Auswirkungen	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle ▪ Durchsicht der Dokumentation zur Änderungskontrolle	☐	☐	☐	☐	☐
6.4.5.2	Dokumentation der Genehmigung durch autorisierte Parteien	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle ▪ Durchsicht der Dokumentation zur Änderungskontrolle	☐	☐	☐	☐	☐
6.4.5.3	(a) Funktionstests, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle ▪ Durchsicht der Dokumentation zur Änderungskontrolle	☐	☐	☐	☐	☐
	(b) Bei benutzerspezifischen Codeänderungen: Testen der Updates auf ihre Konformität mit der PCI-DSS-Anforderung 6.5, bevor sie in der Produktionsumgebung implementiert werden	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle ▪ Durchsicht der Dokumentation zur Änderungskontrolle	☐	☐	☐	☐	☐
6.4.5.4	Back-Out-Verfahren	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle ▪ Durchsicht der Dokumentation zur Änderungskontrolle	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
6.4.6	Werden alle relevanten PCI-DSS-Anforderungen nach Abschluss einer signifikanten Änderung auf allen neuen oder veränderten Systemen und Netzwerken implementiert und die Dokumentation entsprechend aktualisiert? ***Hinweis:*** *Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle ▪ Durchsicht der Dokumentation zur Änderungskontrolle ▪ Mitarbeiter befragen ▪ Beobachten betroffener Systeme oder Netzwerke	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.5	(a) Wird in Softwareentwicklungsprozessen auf häufige Sicherheitsrisiken bei der Programmierung eingegangen?	▪ Richtlinien und Verfahren zur Softwareentwicklung überprüfen	☐	☐	☐	☐	☐
	(b) Werden Entwickler midestens alljährlich auf aktuelle Techniken zum sicheren Codieren, einschließlich dem Vorbeugen häufiger Schwachstellen, geschult?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Schulungsdokumentation überprüfen	☐	☐	☐	☐	☐
	(c) Werden Anwendungen nach Leitlinien zur sicheren Codierung entwickelt, sodass sie mindestens vor folgenden Sicherheitsrisiken geschützt sind? ***Hinweis:*** *Die unter 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken entsprachen zum Zeitpunkt der Veröffentlichung dieser Version des PA-DSS den bewährten Verfahren der Branche. Da jedoch die bewährten Verfahren der Branche beim Management von Sicherheitsrisiken aktualisiert werden (z. B. der Open Web Application Security Project (OWASP) Guide (OWASP-Leitfaden), SANS CWE Top 25, CERT Secure Coding usw.), müssen für diese Anforderungen die aktuellen bewährten Verfahren angewendet werden.*						
6.5.1	Zielen die Codierungsverfahren auf die Vermeidung von Injektionsfehlern, insbesondere bei der SQL-Injektion, ab? ***Hinweis:*** *Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.*	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
6.5.2	Zielen die Codierungsverfahren auf die Vermeidung von Pufferüberläufen ab?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.5.3	Wird in Codierungsverfahren auf unsicheren kryptographischen Speicher eingegangen?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
6.5.4	Wird in Codierungsverfahren auf unsichere Kommunikation eingegangen?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
6.5.5	Wird in Codierungsverfahren auf unsachgemäße Fehlerbehandlung eingegangen?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
6.5.6	Wird in Codierungsverfahren auf alle identifizierten „schwerwiegenden“ Sicherheitsrisiken eingegangen (gemäß PCI-DSS-Anforderung 6.1)?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
Bei Web-Anwendungen und Anwendungsschnittstellen (intern und extern): Werden Anwendungen nach Leitlinien zur sicheren Codierung entwickelt, sodass sie zusätzlich vor den folgenden Sicherheitsrisiken geschützt sind?							
6.5.7	Zielen die Codierungsverfahren auf die Vermeidung von Risiken bei siteübergreifendem Scripting (Cross-Site Scripting XSS) ab?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.5.8	Zielen die Codierungsverfahren auf die Kontrolle unangemessener Zugriffe (z. B. unsichere direkte Objektverweise, fehlende Einschränkung des URL-Zugriffs, Directory Traversal und fehlende Einschränkung des Benutzerzugriffs auf bestimmte Funktionen) ab?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
6.5.9	Zielen die Codierungsverfahren auf die Vermeidung von websiteübergreifender Anfragenfälschung (Cross-Site Request Forgery, CSRF) ab?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
6.5.10	Zielen die Codierungsverfahren auf die Vermeidung einer geknackten Authentifizierungs- und Sitzungsverwaltung ab?	▪ Richtlinien und Verfahren zur Softwareentwicklung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
6.6	Werden alle öffentlichen Webanwendungen regelmäßig von neuen Bedrohungen und Schwachstellen befreit und werden diese Anwendungen vor bekannten Angriffen geschützt, indem *eine* der folgenden Methoden angewendet wird? ▪ Überprüfungen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit: – Mindestens jährlich – Nach jeder Änderung – Durch ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist – In den Bewertungen sollten mindestens die in der Anforderung 6.5 aufgeführten Sicherheitsrisiken überprüft werden. – Dass alle Sicherheitslücken geschlossen werden – Dass die Anwendung nach den Korrekturen erneut bewertet wird ***Hinweis**: Diese Bewertung ist nicht mit den für Anforderung 11.2 durchgeführten Schwachstellenprüfungen identisch.* **– ODER –** ▪ Installation einer automatisierten technischen Lösung, die webbasierte Angriffe (zum Beispiel die Firewall einer Web-Anwendung) wie folgt erkennt und abwehrt: – Die Lösung befindet sich vor öffentlichen Webanwendungen und dient dazu, webbasierte Angriffe zu erkennen und zu verhindern. – Die Lösung wird aktiv ausgeführt und auf dem neuesten Stand gehalten. – In der Lösung werden Prüfprotokolle erstellt. – Die Lösung ist so konfiguriert, dass webbasierte Angriffe abgeblockt werden oder ein Alarm ausgelöst wird, welcher sofort untersucht wird.	▪ Dokumentierte Prozesse überprüfen ▪ Mitarbeiter befragen ▪ Unterlagen zur Bewertung der Anwendungssicherheit untersuchen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
6.7	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Entwicklung und Pflege sicherer Systeme und Anwendungen …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
7.1	Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten wie folgt ausschließlich auf jene Personen beschränkt, deren Tätigkeit diesen Zugriff erfordert?						
	▪ Liegt eine schriftliche Richtlinie zur Zugriffskontrolle vor, die Folgendes vorsieht? • Jeder Rolle werden Zugriffsanforderungen und -berechtigungen zugewiesen. • Der Zugriff für Benutzer-IDs ist auf Mindestberechtigungen, die zum Ausüben der tätigkeitsbezogenen Verpflichtungen erforderlich sind, beschränkt. • Die Zuweisung von Zugriffsberechtigungen basiert auf der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter. • Genehmigungen (in schriftlicher oder elektronischer Form) durch autorisierten Parteien müssen für alle Zugriffsberechtigungen, einschließlich einer Liste der genehmigten Berechtigungen, dokumentiert werden.	▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen	☐	☐	☐	☐	☐
7.1.1	Sind Zugriffsanforderungen für die einzelnen Rollen unter Berücksichtigung der folgenden Aspekte definiert? ▪ Systemkomponenten und Datenressourcen, die für die Ausführung der tätigkeitsbezogenen Funktionen benötigt werden ▪ Erforderliche Berechtigungsstufe (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen	▪ Rollen und Zugriffsanforderungen überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
7.1.2	Ist der Zugriff auf privilegierte Benutzer-IDs wie folgt beschränkt? ▪ Auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind ▪ Exklusive Zuweisung zu Rollen, die diesen privilegierten Zugriff konkret benötigen	▪ Mitarbeiter befragen ▪ Management befragen ▪ Privilegierte Benutzer-IDs überprüfen	☐	☐	☐	☐	☐
7.1.3	Werden Zugriffsberechtigungen anhand der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter zugewiesen?	▪ Management befragen ▪ Benutzer-IDs überprüfen	☐	☐	☐	☐	☐
7.1.4	Wird die dokumentierte Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind, vorausgesetzt?	▪ Benutzer-IDs überprüfen ▪ Mit dokumentierten Genehmigungen vergleichen ▪ Zugewiesene Berechtigungen mit dokumentierten Genehmigungen vergleichen	☐	☐	☐	☐	☐
7.2	Besteht für Systemkomponenten ein Zugriffskontrollsystem, um den Zugriff anhand des Informationsbedarfs eines Benutzers zu beschränken, und ist dieses System wie folgt auf „Alle ablehnen“ eingestellt, sofern der Zugriff nicht ausdrücklich genehmigt wurde?						
7.2.1	Wurden auf allen Systemkomponenten Zugriffskontrollsysteme implementiert?	▪ Anbieterdokumentation durchgehen ▪ Konfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
7.2.2	Wurden die Zugriffskontrollsysteme konfiguriert, um Berechtigungen durchzusetzen, die einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen sind?	▪ Anbieterdokumentation durchgehen ▪ Konfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
7.2.3	Weisen die Zugriffskontrollsysteme die Standardeinstellung „Alle ablehnen“ auf?	▪ Anbieterdokumentation durchgehen ▪ Konfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
7.3	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des Zugriffs auf Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Anforderung 8: Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
8.1	Wurden Richtlinien und Verfahren für Benutzerauthentifizierungs- und Authentifizierungsverwaltungskontrollen für Nichtverbraucher und Administratoren auf allen Systemkomponenten wie folgt implementiert?						
8.1.1	Wurde allen Benutzern eine eindeutige ID zugewiesen, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wurde?	▪ Kennwortverfahren überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
8.1.2	Werden Erweiterungen, Löschungen oder Änderungen von Benutzer-IDs, Berechtigungen oder anderen Identifizierungsobjekten kontrolliert, sodass Benutzer-IDs nur im Rahmen ihrer zugehörigen Genehmigung implementiert werden (einschließlich der angegebenen Rechte)?	▪ Kennwortverfahren überprüfen ▪ IDs der berechtigten und allgemeinen Benutzer sowie zugehörige Autorisierungen überprüfen ▪ Systemeinstellungen prüfen	☐	☐	☐	☐	☐
8.1.3	Wird der Zugriff ehemaliger Benutzer sofort deaktiviert oder entfernt?	▪ Kennwortverfahren überprüfen ▪ Deaktivierte Benutzerkonten untersuchen ▪ Aktuelle Zugriffslisten überprüfen ▪ Zurückgegebene physische Authentifizierungsgeräte überprüfen	☐	☐	☐	☐	☐
8.1.4	Werden Benutzerkonten innerhalb von 90 Tagen entfernt oder deaktiviert?	▪ Kennwortverfahren überprüfen ▪ Benutzerkonten prüfen	☐	☐	☐	☐	☐
8.1.5	(a) Werden Konten von Dritten genutzt, um Systemkomponenten per Fernzugriff aufzurufen, zu unterstützen oder zu pflegen, wobei der Fernzugriff ausschließlich in dem Zeitraum aktiviert ist, in dem er benötigt wird?	▪ Kennwortverfahren überprüfen ▪ Mitarbeiter befragen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Werden die Fernzugriffskonten von Dritten während der Nutzung überwacht?	▪ Mitarbeiter befragen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
8.1.6	(a) Werden wiederholte Zugriffsversuche begrenzt, indem die Benutzer-ID nach mehr als sechs Versuchen ausgesperrt wird?	▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
	(b) *Dieses Testverfahren gilt nur für Dienstanbieter.*						
8.1.7	Wird die Dauer der Sperre eines Benutzerkontos auf mindestens 30 Minuten festgelegt oder bis die Benutzer-ID durch den Administrator wieder freigeschaltet wird?	▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
8.1.8	Müssen sich Benutzer nach einer mehr als 15-minütigen Inaktivität erneut authentifizieren (z. B. indem sie das Kennwort erneut eingeben), um das Terminal oder die Sitzung zu reaktivieren?	▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
8.2	Werden neben der Zuweisung einer eindeutigen ID eine oder mehrere der folgenden Methoden eingesetzt, um alle Benutzer zu authentifizieren? ▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; ▪ etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; ▪ etwas, das Sie sind, wie zum Beispiel biometrische Daten.	▪ Kennwortverfahren überprüfen ▪ Authentifizierungsprozesse überprüfen	☐	☐	☐	☐	☐
8.2.1	(a) Wird auf sämtlichen Systemkomponenten eine starke Verschlüsselung verwendet, um Authentifizerungsangaben (etwa Kennwörter/Kennsätze) während der Übertragung und Speicherung unleserlich zu machen?	▪ Kennwortverfahren überprüfen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationseinstellungen untersuchen ▪ Kennwortdateien überprüfen ▪ Datenübertragungen überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) *Dieses Testverfahren gilt nur für Dienstanbieter.*						
8.2.2	Wird vor der Änderung von Authentifizierungsdaten die Benutzeridentität geprüft (beispielsweise beim Zurücksetzen von Kennwörtern, bei der Bereitstellung neuer Tokens oder bei der Erstellung neuer Schlüssel)?	▪ Authentifizierungsverfahren überprüfen ▪ Mitarbeiter beobachten	☐	☐	☐	☐	☐
8.2.3	(a) Sind Parameter für Benutzerkennwörter so konfiguriert, dass die Kennwörter/-sätze folgende Voraussetzungen erfüllen müssen? • Kennwörter müssen mindestens sieben Zeichen umfassen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden. Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.	▪ Systemkonfigurationseinstellungen zur Überprüfung der Kennwortparameter untersuchen	☐	☐	☐	☐	☐
	(b) *Dieses Testverfahren gilt nur für Dienstanbieter.*						
8.2.4	(a) Werden Benutzerkennwörter/-sätze mindestens alle 90 Tage geändert?	▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
	(b) *Dieses Testverfahren gilt nur für Dienstanbieter.*						
8.2.5	(a) Muss eine Person ein neues Kennwort/einen neuen Kennsatz einreichen, das/der sich von ihren letzten vier Kennwörtern/-sätzen unterscheidet?	▪ Kennwortverfahren überprüfen ▪ Systemkomponenten anhand von Stichproben überprüfen ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
	(b) *Dieses Testverfahren gilt nur für Dienstanbieter.*						

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
8.2.6	Werden Kennwörter/-sätze zur erstmaligen Nutzung und beim Zurücksetzen für jeden Benutzer auf einen eindeutigen Wert gesetzt, und muss jeder Benutzer sein Kennwort sofort nach der ersten Verwendung ändern?	▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen ▪ Sicherheitspersonal beobachten	☐	☐	☐	☐	☐
8.3	Sind alle Nichtkonsolen-Verwaltungszugriffe und alle Fernzugriffe auf das CDE wie folgt durch Multi-Faktor-Authentifizierung geschützt: ***Hinweis:*** *Bei der Multi-Faktor-Authentifizierung müssen mindestens zwei der drei Authentifizierungsmethoden (siehe PCI-DSS-Anforderung 8.2 für eine Beschreibung der Authentifizierungsmethoden) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Multi-Faktor-Authentifizierung.*						
8.3.1	Ist die Multi-Faktor-Authentifizierung fester Bestandteil für alle Nichtkonsolen-Zugriffe auf das CDE durch Mitarbeiter mit Verwaltungszugriff? ***Hinweis:*** *Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*	▪ Systemkonfigurationen untersuchen ▪ Beobachten von Administratoren bei der Anmeldung in die CDE	☐	☐	☐	☐	☐
8.3.2	Ist die Multi-Faktor-Authentifizierung ein fester Bestandteil bei allen Fernzugriffen auf das Netzwerk durch interne Mitarbeiter (Benutzer und Administratoren) und Dritte von außerhalb des Netzwerkes (einschließlich Anbieterzugriff zu Support- oder Wartungszwecken)?	▪ Systemkonfigurationen untersuchen ▪ Beobachten von Mitarbeitern mit Fernzugriff	☐	☐	☐	☐	☐
8.4	(a) Werden Authentifizierungsverfahren und -richtlinien dokumentiert und an alle Benutzer weitergegeben?	▪ Richtlinien und Verfahren durchgehen ▪ Verteilungsmethode überprüfen ▪ Mitarbeiter befragen ▪ Benutzer befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(b) Sind folgende Punkte in den Authentifizierungsverfahren und -richtlinien enthalten? • Hinweise zur Auswahl starker Authentifizierungsinformationen • Hinweise zum Schutz der Authentifizierungsinformationen durch die Benutzer • Anweisungen zur Vermeidung wiederverwendeter Kennwörter • Anweisungen zur Änderung von Kennwörtern beim Verdacht einer Gefährdung	▪ Richtlinien und Verfahren durchgehen ▪ Dokumentation für Benutzer überprüfen	☐	☐	☐	☐	☐
8.5	Sind Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden wie folgt untersagt? • Allgemeine Benutzer-IDs und -konten wurden deaktiviert oder entfernt; • es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen; und • es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.	▪ Richtlinien und Verfahren durchgehen ▪ Benutzer-ID-Listen überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
8.5.1	*Diese Anforderung gilt nur für Dienstanbieter.*						

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
8.6	Wird bei der Anwendung anderer Authentifizierungsmethoden (z. B. Tokens für die physische/logische Sicherheit, Smartcards, Zertifikate usw.) die folgende Zuweisung beachtet? • Authentifizierungsinformationen müssen einem einzelnen Konto zugewiesen sein und dürfen nicht von mehreren Konten gemeinsam genutzt werden. • Mit physischen und/oder logischen Kontrollen muss gewährleistet werden, dass der Zugriff nur über das Konto erfolgen kann, für das die Authentifizierungsinformationen gedacht sind.	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Systemkonfigurationseinstellungen und/oder physische Kontrollen überprüfen	☐	☐	☐	☐	☐
8.7	Der gesamte Zugriff auf die Datenbank mit den Karteninhaberdaten (einschließlich des Zugriffs durch Anwendungen, Administratoren und alle anderen Benutzer) wird wie folgt beschränkt:						
	(a) Erfolgen sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank (z. B. Verschieben, Kopieren und Löschen) ausschließlich programmgesteuert (z. B. über gespeicherte Verfahren)?	▪ Richtlinien und Verfahren zur Datenbankauthentifizierung überprüfen ▪ Konfigurationseinstellungen der Datenbank und Anwendung überprüfen	☐	☐	☐	☐	☐
	(b) Ist der Direktzugriff oder die Datenbankabfrage den Datenbankadministratoren vorbehalten?	▪ Richtlinien und Verfahren zur Datenbankauthentifizierung überprüfen ▪ Zugriffskontrolleinstellungen für die Datenbank überprüfen ▪ Konfigurationseinstellungen der Datenbankanwendung überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(c) Können Anwendungs-IDs nur von den Anwendungen (und nicht von Einzelbenutzern oder anderen Prozessen) verwendet werden?	▪ Richtlinien und Verfahren zur Datenbankauthentifizierung überprüfen ▪ Zugriffskontrolleinstellungen für die Datenbank überprüfen ▪ Konfigurationseinstellungen der Datenbankanwendung überprüfen	☐	☐	☐	☐	☐
8.8	Sind die Sicherheitsrichtlinien und betrieblichen Verfahren zur Identifizierung und Authentifizierung …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
9.1	Wurden angemessene Zugangskontrollen implementiert, um den physischen Zugriff auf Systeme in der Karteninhaberdaten-Umgebung zu überwachen und zu beschränken?	▪ Physische Zugangskontrollen überprüfen ▪ Mitarbeiter beobachten	☐	☐	☐	☐	☐
9.1.1	(a) Wird der Zugang zu sensiblen Bereichen entweder mithilfe von Videokameras und/oder Kontrollsystemen (oder beidem) überwacht? ***Hinweis:*** *„Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die öffentlichen Bereiche, in denen lediglich POS-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).*	▪ Richtlinien und Verfahren durchgehen ▪ Physische Kontrollsysteme überprüfen ▪ Sicherheitsfunktionen überprüfen	☐	☐	☐	☐	☐
	(b) Sind entweder die Videokameras und/oder Zugangskontrollsysteme (oder beides) vor Manipulation oder Deaktivierung geschützt?	▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
	(c) Werden die anhand von Videokameras und/oder Zugangskontrollmechanismen erfassten Daten überprüft und mit anderen Eingaben verglichen?	▪ Richtlinien und Verfahren durchgehen ▪ Sicherheitspersonal befragen	☐	☐	☐	☐	☐
	(d) Werden die anhand von Videokameras und/oder Zugangskontrollmechanismen erfassten Daten mindestens für einen Zeitraum von drei Monaten gespeichert, sofern keine anderweitige gesetzliche Regelung zutrifft?	▪ Prozesse zur Aufbewahrung von Daten überprüfen ▪ Datenspeicherung überprüfen ▪ Sicherheitspersonal befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
9.1.2	Sind physische und/oder logische Kontrollen zur Beschränkung des Zugriffs auf öffentlich zugängliche Netzwerkbuchsen implementiert? *Beispielsweise sollte die Möglichkeit bestehen, Netzwerkbuchsen in für Besucher zugänglichen Bereichen zu deaktivieren und nur dann zu aktivieren, wenn der Netzwerkzugriff ausdrücklich zugelassen ist. Alternativ können auch Prozesse implementiert werden, mit denen Besucher jederzeit in Bereiche mit aktiven Netzwerkbuchsen geleitet werden.*	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Orte beobachten	☐	☐	☐	☐	☐
9.1.3	Ist der physische Zugriff auf WLAN-Zugriffspunkte, Gateways, Handheld-Geräte, Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen beschränkt?	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Geräte überprüfen	☐	☐	☐	☐	☐
9.2	(a) Wurden Verfahren entwickelt, die die Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern erleichtern, und wurden dabei folgende Punkte berücksichtigt? • Identifizierung von Besuchern und Mitarbeitern vor Ort (z. B. durch Vergabe von Ausweisen), • Zugangs- bzw. Zugriffsanforderungen und • Rücknahme der Identifizierung (z. B. mittels Ausweis) von ehemaligen Vor-Ort-Mitarbeitern und Besuchern, deren Besuchsstatus abgelaufen ist *Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Mitarbeiter vor Ort" hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und Subunternehmen sowie Berater, die am Standort der jeweiligen Stelle arbeiten. Ein „Besucher" wird als Lieferant, Gast eines Mitarbeiters vor Ort, Servicemitarbeiter oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag.*	▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Identifizierungsmethoden überprüfen (z. B. Ausweise) ▪ Besucherprozesse überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Werden Besucher anhand von Identifizierungsmethoden (z. B. Ausweise) klar identifiziert und sind sie leicht von den Mitarbeitern vor Ort zu unterscheiden?	▪ Identifizierungsmethoden überprüfen	☐	☐	☐	☐	☐
	(c) Ist der Zugriff auf das Ausweissystem ausschließlich befugtem Personal vorbehalten?	▪ Physische Kontrollen und Zugangskontrollen für das Ausweissystem überprüfen	☐	☐	☐	☐	☐
9.3	Wird der Zugang von Vor-Ort-Personal zu den sensiblen Bereichen gemäß den folgenden Anforderungen kontrolliert? ▪ Ist der Zugang autorisiert und basiert er auf der jeweiligen tätigkeitsbezogenen Aufgabe? ▪ Wird der Zugang nach dem Ende der Beschäftigung umgehend deaktiviert? ▪ Werden nach dem Ende der Beschäftigung sämtliche physischen Zugangssysteme wie Schlüssel oder Karten zurückgegeben oder deaktiviert?	▪ Mitarbeiter befragen ▪ Zugangskontrolllisten überprüfen ▪ Mitarbeiter vor Ort beobachten ▪ Listen ausgeschiedener Mitarbeiter mit Zugangskontrolllisten vergleichen	☐	☐	☐	☐	☐
9.4	Werden die Identifizierung und der Zugang der Besucher wie folgt gehandhabt?						
9.4.1	Werden die Besucher vor dem Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden, autorisiert und innerhalb dieser Bereiche jederzeit begleitet?	▪ Richtlinien und Verfahren durchgehen ▪ Besucherprozesse einschließlich Art der Zugangskontrolle überprüfen ▪ Mitarbeiter befragen ▪ Besucher und Ausweisnutzung beobachten	☐	☐	☐	☐	☐
9.4.2	(a) Werden die Besucher identifiziert und mit einem Ausweis oder einer sonstigen Identifizierung versehen, mit der sie sich deutlich von den Vor-Ort-Mitarbeitern unterscheiden lassen?	▪ Ausweisnutzung von Mitarbeitern und Besuchern beobachten ▪ Identifizierung überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Sind Besucherausweise oder sonstige Formen der Identifizierung befristet?	▪ Prozess überprüfen ▪ Identifizierung überprüfen	☐	☐	☐	☐	☐
9.4.3	Werden die Besucher um Rückgabe oder Deaktivierung des Ausweises bzw. anderer Identifizierungsmöglichkeiten gebeten, wenn sie die Einrichtung verlassen oder die Erlaubnis abläuft?	▪ Prozesse überprüfen ▪ Besucher, die die Einrichtung verlassen, beobachten	☐	☐	☐	☐	☐
9.4.4	(a) Gibt es ein Besucherprotokoll, in dem der Zugang zur Einrichtung sowie zu den Computerräumen und Rechenzentren, in denen Karteninhaberdaten gespeichert oder übertragen werden, protokolliert wird?	▪ Richtlinien und Verfahren durchgehen ▪ Besucherprotokoll überprüfen ▪ Besucherprozesse überprüfen ▪ Aufbewahrung des Protokolls überprüfen	☐	☐	☐	☐	☐
	(b) Enthält das Besucherprotokoll den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der dem Besucher Zugang gewährt?	▪ Richtlinien und Verfahren durchgehen ▪ Besucherprotokoll überprüfen	☐	☐	☐	☐	☐
	(c) Wird das Besucherprotokoll mindestens drei Monate aufbewahrt?	▪ Richtlinien und Verfahren durchgehen ▪ Aufbewahrung des Besucherprotokolls überprüfen	☐	☐	☐	☐	☐
9.5	Wird die physische Sicherheit aller Medien gewährleistet (insbesondere Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)? *Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Medien" auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.*	▪ Richtlinien und Verfahren zur physischen Sicherung von Medien durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
9.5.1		▪	☐	☐	☐	☐	☐
	Wird der Standort, an dem die Sicherheitskopien der Medien gespeichert werden, mindest einmal im Jahr überprüfen, um zu bestätigen, dass dieser sicher ist?	▪ Richtlinien und Verfahren zur Überprüfung externer Datenträgerstandorte untersuchen ▪ Sicherheitspersonal befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
9.6	(a) Wird die interne oder externe Verteilung jeglicher Art von Medien stets strikt kontrolliert?	▪ Richtlinien und Verfahren zur Verteilung von Medien durchgehen	☐	☐	☐	☐	☐
	(b) Umfassen die Kontrollen folgende Punkte?						
9.6.1	Werden Medien klassifiziert, sodass die Sensibilität der Daten bestimmt werden kann?	▪ Richtlinien und Verfahren zur Klassifizierung von Medien durchgehen ▪ Sicherheitspersonal befragen	☐	☐	☐	☐	☐
9.6.2	Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?	▪ Mitarbeiter befragen ▪ Protokolle und Dokumentation zur Verteilung von Medien untersuchen	☐	☐	☐	☐	☐
9.6.3	Wird vor dem Verlagern von Medien die Genehmigung des Managements eingeholt (insbesondere wenn Medien an Einzelpersonen verteilt werden)?	▪ Mitarbeiter befragen ▪ Protokolle und Dokumentation zur Verteilung von Medien untersuchen	☐	☐	☐	☐	☐
9.7	Werden strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durchgeführt?	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
9.7.1	(a) Werden Inventurlisten aller Medien ordnungsgemäß geführt?	▪ Inventurlisten überprüfen	☐	☐	☐	☐	☐
	(b) Findet mindestens einmal pro Jahr eine Inventur der vorhandenen Medien statt?	▪ Inventurlisten überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
9.8	(a) Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen	☐	☐	☐	☐	☐
	(b) Gibt es eine Richtlinie zur regelmäßigen Vernichtung von Medien, in der folgende Anforderungen definiert sind? • Ausdrucke müssen der Aktenvernichtung zugeführt werden, damit nach allgemeinem Ermessen ausgeschlossen werden kann, dass die Einzelteile wieder zusammengefügt werden. • Container zur Aufbewahrung von zu vernichtendem Material müssen geschützt werden. • Karteninhaberdaten auf elektronischen Medien müssen nach Branchenstandards z. B. über Secure Wipes (sichere Löschverfahren) in einen Zustand versetzt werden, in dem sie nicht wiederherstellbar sind. Ersatzweise können auch die Medien physisch unbrauchbar gemacht werden.	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen	☐	☐	☐	☐	☐
	(c) Erfolgt die Vernichtung von Medien wie nachstehend beschrieben?						
9.8.1	(a) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?	▪ Mitarbeiter befragen ▪ Verfahren untersuchen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
	(b) Werden Container zur Aufbewahrung von zu vernichtenden Informationen so geschützt, dass Zugriffe auf diese Inhalte vermieden werden?	▪ Sicherheit von Containern überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
9.8.2	Werden Karteninhaberdaten auf elektronischen Medien nach Branchenstandards unbrauchbar und nicht wiederherstellbar gemacht bzw. anderweitig unbrauchbar gemacht, indem die Medien vernichtet werden, damit keine Karteninhaberdaten wiederhergestellt werden können (z. B. durch ein Secure-Wipe-Programm)?	▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
9.9	Sind die Geräte, die Zahlungskartendaten über eine direkte physische Interaktion mit der Karte erfassen, vor Manipulation und Austausch geschützt? ***Hinweis:*** *Diese Anforderung gilt für Kartenlesegeräte, die bei Transaktionen eingesetzt werden, bei denen die Karte am Point-of-Sale vorliegt und durch das Gerät gezogen oder in das Gerät eingesteckt werden muss. Diese Anforderung gilt nicht für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke.*						
	(a) Sehen Richtlinien und Verfahren das Führen einer Liste solcher Geräte vor?	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
	(b) Sehen Richtlinien und Verfahren vor, dass Geräte regelmäßig auf Manipulations- oder Austauschversuche untersucht werden?	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
	(c) Sehen Richtlinien und Verfahren vor, dass das Bewusstsein der Mitarbeiter für verdächtiges Verhalten und das Melden der Manipulation bzw. des Austauschs von Geräten gefördert werden?	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
9.9.1	(a) Enthält die Geräteliste folgende Angaben? • Fabrikat und Modell des Geräts • Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet) • Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung	▪ Geräteliste überprüfen	☐	☐	☐	☐	☐
	(b) Ist die Liste korrekt, vollständig und aktuell?	▪ Geräte und Gerätestandorte beobachten und mit der Liste vergleichen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(c) Wird die Geräteliste aktualisiert, sobald Geräte hinzugefügt, an einen anderen Standort gebracht, außer Betrieb genommen werden usw.?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
9.9.2	(a) Werden Geräteoberflächen regelmäßig auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch untersucht (stimmen beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht?)? ***Hinweis:*** *Anzeichen für eine Manipulation oder den Austausch von Geräten sind zum Beispiel unerwartete Anbauten oder Kabel, fehlende oder geänderte Sicherheitssiegel, beschädigte oder andersfarbige Gehäuse bzw. Änderungen bei der Seriennummer oder anderen externen Kennzeichen.*	▪ Mitarbeiter befragen ▪ Untersuchungsprozesse beobachten und mit festgelegten Prozessen vergleichen	☐	☐	☐	☐	☐
	(b) Kennen die Mitarbeiter die Verfahren zur Untersuchung von Geräten?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
9.9.3	Wurde das Bewusstsein der Mitarbeiter für Manipulations- oder Austauschversuche insbesondere durch die nachfolgenden Punkte gefördert?						
	(a) Umfasst das Schulungsmaterial für die Mitarbeiter an POS-Standorten die folgenden Punkte? • Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten). • Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe. • Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen). • Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter).	▪ Schulungsmaterialien überprüfen	☐	☐	☐	☐	☐
	(b) Wurden die Mitarbeiter an POS-Standorten geschult und haben sie die Verfahren zur Erkennung und Meldung von Versuchen der Manipulation oder des Austauschs von Geräten verinnerlicht?	▪ Mitarbeiter an POS-Standorten befragen	☐	☐	☐	☐	☐
9.10	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des physischen Zugriffs auf Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
10.1	(a) Sind Audit-Trails für die Systemkomponenten vorhanden und aktiv?	▪ Prozesse überprüfen ▪ Systemadministrator befragen	☐	☐	☐	☐	☐
	(b) Ist der Zugriff auf Systemkomponenten mit den einzelnen Benutzern verknüpft?	▪ Prozesse überprüfen ▪ Systemadministrator befragen	☐	☐	☐	☐	☐
10.2	Werden automatisierte Audit-Trails für alle Systemkomponenten implementiert, um folgende Ereignisse rekonstruieren zu können?						
10.2.1	Alle individuellen Benutzerzugriffe auf Karteninhaberdaten;	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.2.2	Alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommenen Aktionen	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.2.3	Zugriff auf alle Audit-Trails;	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.2.4	Ungültige logische Zugriffsversuche	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
10.2.5	Verwendung und Änderung der Identifizierungs- und Authentifizierungsmechanismen (u. a. bei der Erstellung neuer Konten, Heraufstufung von Rechten usw.) – und sämtliche Änderungen, Ergänzungen und Löschungen an bzw. von Konten mit Root- oder Administratorrechten	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.2.6	Initialisieren, Beenden oder Anhalten der Prüfprotokolle;	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.2.7	Erstellen und Löschen von Objekten auf Systemebene?	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.3	Werden die folgenden Audit-Trail-Einträge für alle Systemkomponenten für jedes Ereignis aufgezeichnet?						
10.3.1	Benutzeridentifizierung	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.3.2	Ereignistyp	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.3.3	Datum und Uhrzeit	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
10.3.4	Erfolgs- oder Fehleranzeige	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.3.5	Ereignisursprung	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.3.6	Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
10.4	Werden alle wichtigen Systemuhren und Zeiten durch den Einsatz von Zeitsynchronisierungstechnologien synchronisiert und werden diese Technologien aktualisiert? ***Hinweis:*** *Eine Zeitsynchronisierungstechnologie ist beispielsweise das Network Time Protocol (NTP).*	▪ Standards und Prozesse der Zeitkonfiguration überprüfen	☐	☐	☐	☐	☐
10.4.1	Werden die folgenden Prozesse umgesetzt, um sicherzustellen, dass in wichtigen Systemen die richtige und identische Zeit eingestellt ist?						
	(a) Empfangen ausschließlich die festgelegten zentralen Zeitserver Zeitsignale von externen Quellen, und basieren diese Zeitsignale auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC)?	▪ Standards und Prozesse der Zeitkonfiguration überprüfen ▪ Zeitbezogene Systemparameter überprüfen	☐	☐	☐	☐	☐
	(b) Wenn es mehrere festgelegte Zeitserver gibt, bestimmen diese Server untereinander die richtige Uhrzeit?	▪ Standards und Prozesse der Zeitkonfiguration überprüfen ▪ Zeitbezogene Systemparameter überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(c) Stammen die Zeitinformationen auf den Systemen ausschließlich von den festgelegten zentralen Zeitservern?	▪ Standards und Prozesse der Zeitkonfiguration überprüfen ▪ Zeitbezogene Systemparameter überprüfen	☐	☐	☐	☐	☐
10.4.2	Werden die Zeitinformationen wie folgt geschützt? (a) Ist der Zugriff auf Zeitinformationen ausschließlich Mitarbeitern vorbehalten, die den Zugriff auf Zeitinformationen aus geschäftlichen Gründen benötigen?	▪ Systemkonfigurationen und Zeitsynchronisierungseinstellungen überprüfen	☐	☐	☐	☐	☐
	(b) Werden Änderungen an den Zeiteinstellungen auf wichtigen Systemen protokolliert, überwacht und überprüft?	▪ Systemkonfigurationen und Zeitsynchronisierungseinstellungen und -protokolle überprüfen	☐	☐	☐	☐	☐
10.4.3	Werden die Zeiteinstellungen von branchenüblichen Zeitquellen empfangen? (Somit wird verhindert, dass böswillige Personen die Uhren ändern können.) *Diese Zeitaktualisierungen können mit einem symmetrischen Schlüssel verschlüsselt werden. Außerdem können Zugriffskontrolllisten erstellt werden, aus denen die IP-Adressen der Client Rechner hervorgehen, die die Zeitaktualisierungen in Anspruch nehmen. (Hierdurch wird die Nutzung nicht autorisierter interner Zeitserver verhindert.)*	▪ Systemkonfigurationen untersuchen	☐	☐	☐	☐	☐
10.5	Werden wie folgt Audit-Trails gesichert, sodass sie nicht geändert werden können?						
10.5.1	Ist die Anzeige der Audit-Trails auf Personen mit arbeitsbedingtem Bedarf beschränkt?	▪ Systemadministratoren befragen ▪ Systemkonfigurationen und -berechtigungen untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
10.5.2	Werden die Dateien von Audit-Trails mit Zugriffskontrollsystemen, räumlicher Trennung und/oder Netzwerktrennung vor unbefugten Änderungen geschützt?	▪ Systemadministratoren befragen ▪ Systemkonfigurationen und -berechtigungen untersuchen	☐	☐	☐	☐	☐
10.5.3	Werden Audit-Trail-Dateien unverzüglich auf einem zentralisierten Protokollserver oder auf Medien gesichert, die nur schwer zu manipulieren sind?	▪ Systemadministratoren befragen ▪ Systemkonfigurationen und -berechtigungen untersuchen	☐	☐	☐	☐	☐
10.5.4	Werden Protokolle für nach außen gerichtete Technologien (z. B. Wireless-Systeme, Firewalls, DNS, E-Mail) auf sicheren, zentralen und internen Protokollservern oder Medien abgelegt?	▪ Systemadministratoren befragen ▪ Systemkonfigurationen und -berechtigungen untersuchen	☐	☐	☐	☐	☐
10.5.5	Werden für die Protokolle verschiedene Datei-Integritätsüberwachungs- und Änderungserfassungssoftware verwendet, um zu gewährleisten, dass bestehende Protokolldaten nicht geändert werden können, ohne dass Alarme ausgelöst werden (obgleich neue Daten ohne Auslösung von Alarmen hinzugefügt werden können)?	▪ Einstellungen, überwachte Dateien und Ergebnisse aus Überwachungen untersuchen	☐	☐	☐	☐	☐
10.6	Werden Protokolle und Sicherheitsereignisse für alle Systemkomponenten auf Unregelmäßigkeiten oder verdächtige Aktivitäten überprüft? ***Hinweis:*** *Um die Konformität mit Anforderung 10.6 zu erzielen, können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.*						

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
10.6.1	(a) Sind schriftliche Richtlinien und Verfahren zur mindestens täglichen Überprüfung – manuell oder mithilfe von Protokolltools – vorhanden? • Sämtliche Sicherheitsereignisse • Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen • Die Protokolle aller wichtigen Systemkomponenten • Die Protokolle aller Server- und Systemkomponenten, die Sicherheitsfunktionen ausführen (z. B. Firewalls, Systeme zur Erkennung/Verhinderung von Eindringversuchen (IDS/IPS), Authentifizierungsserver, E-Commerce-Umleitungsserver usw.)	▪ Sicherheitsrichtlinien und -verfahren durchgehen	☐	☐	☐	☐	☐
	(b) Werden die oben genannten Protokolle und Sicherheitsereignisse mindestens einmal täglich überprüft?	▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
10.6.2	(a) Sind schriftliche Richtlinien und Verfahren vorhanden, wonach eine regelmäßige Prüfung der Protokolle aller anderen Systemkomponenten (manuell oder mittels Protokolltools) auf der Grundlage der Richtlinien und der Risikomanagementstrategie des Unternehmens stattfinden soll?	▪ Sicherheitsrichtlinien und -verfahren durchgehen	☐	☐	☐	☐	☐
	(b) Werden alle anderen Systemkomponenten gemäß den Richtlinien und der Risikomanagementstrategie des Unternehmens überprüft?	▪ Dokumentation zur Risikobeurteilung durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
10.6.3	(a) Sind schriftliche Richtlinien und Verfahren zur Nachverfolgung von Ausnahmen und Unregelmäßigkeiten, die bei der Prüfung ermittelt wurden, vorhanden?	▪ Sicherheitsrichtlinien und -verfahren durchgehen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(b) Werden Ausnahmen und Unregelmäßigkeiten nachverfolgt?	▪ Prozesse überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
10.7	(a) Sind Richtlinien und Verfahren zur Aufbewahrung von Prüfprotokollen vorhanden und sehen sie vor, dass Protokolle mindestens ein Jahr aufbewahrt werden und mindestens drei Monate unmittelbar zur Analyse verfügbar sein müssen (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar)?	▪ Sicherheitsrichtlinien und -verfahren durchgehen	☐	☐	☐	☐	☐
	(b) Werden Prüfprotokolle mindestens ein Jahr aufbewahrt?	▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen	☐	☐	☐	☐	☐
	(c) Sind die Protokolle zu Analysezwecken mindestens drei Monate lang unmittelbar verfügbar?	▪ Mitarbeiter befragen ▪ Prozesse überprüfen	☐	☐	☐	☐	☐
10.8	*Diese Anforderung gilt nur für Dienstanbieter*						
10.9	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Kontrolle des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
11.1	(a) Werden Prozesse zur Erkennung und Identifizierung von autorisierten und nicht autorisierten WLAN-Zugriffspunkten vierteljährlich implementiert? ***Hinweis:*** *Methoden, die sich hierfür anbieten, sind unter anderen Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme.* *Welche Methode auch immer verwendet wird, sie muss ausreichend sein, um jegliche nicht autorisierten Geräte zu erkennen und zu identifizieren.*	▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
	(b) Ist die angewandte Methodik ausreichend, um jegliche nicht autorisierte Zugriffspunkte für drahtlose Netzwerke, einschließlich mindestens folgender Elemente, zu erkennen und zu identifizieren? • In Systemkomponenten eingefügte WLAN-Karten; • an Systemkomponenten angeschlossene tragbare Geräte (z. B. durch USB), mit denen ein WLAN-Zugriffspunkt eingerichtet wird; und • an einen Netzwerkport oder ein Netzwerkgerät angeschlossene Drahtlosgeräte.	▪ Methodik evaluieren	☐	☐	☐	☐	☐
	(c) Werden Wireless-Scans zur Identifizierung nicht autorisierter WLAN-Zugriffspunkte mindestens vierteljährlich auf allen Systemkomponenten und an allen Stellen durchgeführt?	▪ Ergebnisse der letzten WLAN-Untersuchungen überprüfen	☐	☐	☐	☐	☐
	(d) Falls eine automatische Überwachung eingesetzt wird (z. B. ein Wireless IDS/IPS-System, NAC usw.), sind in der Konfiguration Alarmmeldungen für das Personal vorgesehen?	▪ Konfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
11.1.1	Werden die autorisierten WLAN-Zugriffspunkte inventarisiert und ist zu jedem Zugriffspunkt eine geschäftliche Begründung dokumentiert?	▪ Inventar und Unterlagen überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
11.1.2	(a) Ist im Vorfallreaktionsplan eine Reaktion für den Fall definiert und vorgesehen, dass ein nicht autorisierter WLAN-Zugriffspunkt entdeckt wird?	▪ Vorfallreaktionsplan untersuchen (siehe Anforderung 12.10)	☐	☐	☐	☐	☐
	(b) Werden Maßnahmen getroffen, wenn nicht autorisierte WLAN-Zugriffspunkte gefunden werden?	▪ Verantwortliche Mitarbeiter befragen ▪ Letzte WLAN-Untersuchungen (Scans) und daraufhin erfolgte Reaktionen überprüfen	☐	☐	☐	☐	☐
11.2	Werden wie folgt interne und externe Netzwerkanfälligkeits-Scans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Modifizierungen von Firewall-Regeln, Produktupgrades) ausgeführt? ***Hinweis:*** *Um beim vierteljährlichen Scan sämtliche Systeme und alle möglichen Sicherheitsrisiken zu berücksichtigen, können mehrere Scan-Berichte miteinander kombiniert werden. Es ist unter Umständen zusätzliche Dokumentation erforderlich, um zu belegen, dass bei noch nicht behobenen Sicherheitsrisiken erste Schritte unternommen wurden.* *Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier vierteljährliche Scans bestanden sein müssen, wenn der Prüfer feststellt, dass 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Einheit über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle in den Scan-Ergebnissen festgestellten Sicherheitsrisiken nachweislich korrigiert wurden. Für die Folgejahre nach der ersten PCI-DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.*						
11.2.1	(a) Werden vierteljährlich interne Schwachstellenprüfungen durchgeführt?	▪ Scan-Berichte durchgehen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Behandelt der vierteljährliche interne Scanprozess alle „schwerwiegenden“ Sicherheitslücken und sieht erneute Scans vor, bis diese (gemäß PCI-DSS-Anforderung 6.1) gelöst wurden?	▪ Scan-Berichte durchgehen	☐	☐	☐	☐	☐
	(c) Werden die internen vierteljährlichen Scans von (einem) dafür qualifizierten internen Mitarbeiter(n) oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
11.2.2	(a) Werden vierteljährlich externe Schwachstellenprüfungen (Scans) durchgeführt? ***Hinweis:*** *Vierteljährliche externe Schwachstellenprüfungen müssen von einem Scanninganbieter (Approved Scanning Vendor, ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI SSC) zugelassen wurde.* *Informationen zu den Scan-Kunden-Zuständigkeiten, der Scan-Vorbereitung usw. finden Sie im ASV-Programmführer auf der PCI-SSC-Website.*	▪ Ergebnisse der externen Schwachstellenprüfungen aus den vorangegangenen vier Quartalen durchgehen	☐	☐	☐	☐	☐
	(b) Erfüllen die Ergebnisse der vierteljährlichen externen Prüfungen und erneuten Prüfungen die Anforderungen des *ASV-Programmleitfadens* (z. B. keine Schwachstellen, die vom CVSS eine Klassifizierung von 4.0 oder höher erhalten haben und keine automatischen Ausfälle)?	▪ Ergebnisse der vierteljährlichen externen Prüfungen und erneuten Prüfungen durchgehen	☐	☐	☐	☐	☐
	(c) Werden vierteljährliche externe Schwachstellenprüfungen von einem vom PCI SSC zugelassenen Scanninganbieter (Approved Scanning Vendor, ASV) durchgeführt?	▪ Ergebnisse der vierteljährlichen externen Prüfungen und erneuten Prüfungen durchgehen	☐	☐	☐	☐	☐
11.2.3	(a) Werden nach jeder wesentlichen Änderung interne und externe Prüfungen und nach Bedarf erneute Prüfungen durchgeführt? ***Hinweis:*** *Scans müssen von qualifizierten Mitarbeitern durchgeführt werden.*	▪ Änderungskontrolldokumentation und Scan-Berichte überprüfen und zuordnen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
	(b) Sieht der Scanprozess erneute Scans vor, bis … • … bei externen Scans keine Sicherheitsrisiken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung höher als 4.0 bewertet wurden, • … bei internen Scans der Fehler behoben wurde oder alle „schwerwiegenden" Sicherheitslücken, wie in der PCI-DSS-Anforderung 6.1 dargelegt, gelöst wurden?	▪ Scan-Berichte durchgehen	☐	☐	☐	☐	☐
	(c) Werden die Scans von mindestens einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
11.3	Sieht die Methodik für Penetrationstests Folgendes vor? ▪ Die Methodik basiert auf branchenweit akzeptierten Verfahren für Penetrationstests (z. B. NIST SP800-115). ▪ Die Methodik umfasst die gesamte Umgebung der CDE und wichtige Systeme. ▪ Es werden Tests innerhalb und außerhalb des Netzwerks durchgeführt. ▪ Bei den Tests werden auch Kontrollen zur Segmentierung und zur Reduktion des Umfangs validiert. ▪ Bei der Definition von Penetrationstests auf Anwendungsebene müssen mindestens die in Anforderung 6.5 aufgeführten Sicherheitsrisiken berücksichtigt werden. ▪ Es müssen Penetrationstests auf Netzwerkebene definiert werden, die sämtliche Komponenten zur Unterstützung von Netzwerkfunktionen und Betriebssysteme enthalten. ▪ Bei der Methodik müssen die in den letzten 12 Monaten aufgetretenen Bedrohungen und Sicherheitsrisiken berücksichtigt werden. ▪ Es muss festgelegt sein, wo die Ergebnisse von Penetrationstests und Abhilfemaßnahmen gespeichert werden sollen.	▪ Methodik für Penetrationstests untersuchen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
11.3.1	(a) Werden *externe* Penetrationstests mindestens einmal im Jahr und nach sämtlichen signifikanten Infrastruktur- oder Anwendungsänderungen an der Umgebung durchgeführt (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung)?	▪ Arbeitsaufwand untersuchen ▪ Ergebnisse des letzten externen Penetrationstests untersuchen	☐	☐	☐	☐	☐
	(b) Werden die Tests von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
11.3.2	(a) Werden *interne* Penetrationstests mindestens einmal im Jahr und nach sämtlichen signifikanten Infrastruktur- oder Anwendungsänderungen an der Umgebung durchgeführt (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung)?	▪ Arbeitsaufwand untersuchen ▪ Ergebnisse des letzten internen Penetrationstests untersuchen	☐	☐	☐	☐	☐
	(b) Werden die Tests von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
11.3.3	Werden die beim Penetrationstest ermittelten ausnutzbaren Sicherheitsrisiken behoben und wird anschließend ein erneuter Test durchgeführt?	▪ Ergebnisse der Penetrationstests untersuchen	☐	☐	☐	☐	☐
11.3.4	Falls die CDE durch Segmentierung von anderen Netzwerken isoliert wird:						
	(a) Sehen die Penetrationstestverfahren vor, dass alle Segmentierungsmethoden daraufhin geprüft werden, ob sie funktionieren und effektiv sind, und dass alle Systeme außerhalb des Bereichs von den Systemen innerhalb des CDE isoliert werden müssen?	▪ Segmentierungskontrollen überprüfen ▪ Methodik für Penetrationstests überprüfen	☐	☐	☐	☐	☐
	(b) Erfüllen die Penetrationstests zur Überprüfung der Segmentierungskontrollen die folgenden Voraussetzungen? • Die Tests werden mindestens einmal jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt. • Bei den Tests werden alle angewendeten Segmentierungskontrollen/-methoden geprüft. • Es wird geprüft, ob die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden.	▪ Ergebnisse des letzten Penetrationstests untersuchen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(c) Werden die Tests von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
11.3.4.1	*Diese Anforderung gilt nur für Dienstanbieter*						
11.4	(a) Sind Systeme zur Erkennung und/oder Verhinderung von Angriffen auf das Netzwerk vorhanden, um den gesamten Verkehr an folgenden Punkten zu überwachen? • In der Umgebung der CDE und • an kritischen Punkten in der CDE	▪ Systemkonfigurationen untersuchen ▪ Netzwerkdiagramme überprüfen	☐	☐	☐	☐	☐
	(b) Sind Systeme zur Erkennung und/oder Verhinderung von Angriffen auf das Netzwerk so konfiguriert, dass das Personal bei mutmaßlichen Sicherheitsverletzungen alarmiert wird?	▪ Systemkonfigurationen untersuchen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
	(c) Werden Angriffserfassungs- und -vorbeugungssysteme, Standardeinstellungen und Signaturen fortwährend aktualisiert?	▪ IDS/IPS-Konfigurationen untersuchen ▪ Anbieterdokumentation überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
11.5	(a) Wird ein System zur Erkennung von Änderungen (z. B. Tools zur Überwachung der Dateiintegrität) bereitgestellt, um nicht autorisierte Änderungen (einschließlich Änderungen, Ergänzungen und Löschungen) an wichtigen System-, Konfigurations- oder Inhaltsdateien zu erkennen? *Dateien, die überwacht werden sollten, sind u. a.:* • *Ausführbare Systemdateien* • *Ausführbare Anwendungsdateien* • *Konfigurations- und Parameterdateien* • *Zentral gespeicherte Protokoll- und Audit-Dateien (alt oder archiviert)* • *Zusätzliche von der Einheit als wichtig betrachtete Dateien (z. B. aufgrund einer Risikobewertung o. ä.)*	▪ Systemeinstellungen und überwachte Dateien beobachten ▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
	(b) Ist das System zur Erkennung von Änderungen so konfiguriert, dass das Personal über nicht autorisierte Änderungen (einschließlich Änderungen, Ergänzungen und Löschungen) an wichtigen System-, Konfigurations- oder Inhaltsdateien benachrichtigt wird, und führen diese Tools mindestens wöchentlich Vergleiche wichtiger Dateien durch? ***Hinweis:*** *Zum Zwecke der Erkennung von Änderungen sind wichtige Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung aber auf eine Sicherheitsverletzung im System oder auf das Risiko einer Verletzung hinweisen könnte. Systeme zur Änderungserkennung, wie beispielsweise Produkte zur Dateiintegritätsüberwachung, sind in der Regel bereits vorab mit wichtigen Dateien für das jeweilige Betriebssystem konfiguriert. Andere kritische Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstanbieter) beurteilt und definiert werden.*	▪ Systemeinstellungen und überwachte Dateien beobachten ▪ Ergebnisse der Überwachung durchgehen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
11.5.1	Wurde ein Prozess implementiert, um auf Alarme der Änderungserkennungslösung reagieren zu können?	▪ Systemkonfigurationseinstellungen untersuchen	☐	☐	☐	☐	☐
11.6	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Sicherheitsüberwachung und für Tests …? • dokumentiert • derzeit in Verwendung • allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren überprüfen ▪ Mitarbeiter befragen	☐	☐	☐	☐	☐

Befolgung einer Informationssicherheitsrichtlinie

Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.

Hinweis: *Zum Zwecke der Anforderung 12 bezieht sich der Begriff „Mitarbeiter“ hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Stelle „ansässig“ sind oder anderweitig Zugriff auf die Karteninhaberdaten-Umgebung haben.*

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
12.1	Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und an das betroffene Personal weitergeleitet?	▪ Informationssicherheitsrichtlinie überprüfen	☐	☐	☐	☐	☐
12.1.1	Wird die Sicherheitsrichtlinie mindestens einmal pro Jahr überarbeitet und bei Umgebungsänderungen aktualisiert?	▪ Informationssicherheitsrichtlinie überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.2	(a) Wurde ein Prozess zur jährlichen Risikobeurteilung implementiert, der die folgenden Merkmale aufweist • Beim Prozess werden wichtige Ressourcen, Bedrohungen und Sicherheitsrisiken ermittelt. • Führt der Prozess zu einer offiziellen, dokumentierten Risikoanalyse? *Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.*	▪ Jährlichen Risikobewertungsprozess überprüfen ▪ Mitarbeiter befragen ▪	☐	☐	☐	☐	☐
	(b) Wird der Risikobewertungsprozess mindestens einmal im Jahr und nach wesentlichen Änderungen an der Umgebung (z. B. Übernahmen, Fusionen, Umzüge usw.) durchgeführt?	▪ Dokumentation zur Risikobeurteilung durchgehen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
12.3	Wurden Nutzungsrichtlinien für wichtige Technologien entwickelt, um die ordnungsgemäße Nutzung dieser Technologien zu regeln – unter Berücksichtigung der nachfolgenden Punkte? ***Hinweis:*** *Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.*						
12.3.1	Ausdrückliche Genehmigung durch autorisierte Parteien, diese Technologien zu nutzen	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.2	Authentifizierung zur Verwendung der Technologien	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.3	Eine Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.4	Gibt es eine Methode zur genauen und schnellen Bestimmung von Eigentümern, Kontaktinformationen und Zweck (z. B. Etikettierung und Codierung von Geräten sowie Einbuchung in den Bestand)?	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.5	Akzeptable Nutzung dieser Technologien	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.6	Akzeptable Netzwerkorte für die Technologien	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.7	Liste der vom Unternehmen zugelassenen Produkte;	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
12.3.8	Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.9	Aktivierung von Remotezugriff-Technologien für Anbieter und Geschäftspartner nur, wenn bei Anbietern und Geschäftspartnern ein dringender Bedarf besteht und die Technologie nach der Nutzung gleich wieder deaktiviert wird.	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.3.10	(a) Falls Mitarbeiter auf Karteninhaberdaten per Remote-Zugriff zugreifen, wird in der Richtlinie untersagt, Karteninhaberdaten auf lokale Festplatten und elektronische Wechselmedien zu kopieren, zu verschieben oder zu speichern, sofern nicht ausdrücklich aufgrund bekannter Geschäftsbedürfnisse gestattet? *Wenn ein bekanntes geschäftliches Bedürfnis besteht, muss in den Nutzungsrichtlinien festgelegt sein, dass die Daten entsprechend den geltenden PCI-DSS-Anforderungen geschützt werden.*	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
	(b) Sieht die Richtlinie für Mitarbeiter mit entsprechenden Befugnissen den Schutz der Karteninhaberdaten gemäß den PCI-DSS-Anforderungen vor?	▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen ▪ Per Stichprobe ausgewählte Mitarbeiter befragen	☐	☐	☐	☐	☐
12.4.1	*Diese Anforderung gilt nur für Dienstanbieter*						
12.5	(a) Werden die Verantwortlichkeiten in Sachen Sicherheit formal einem Sicherheitsbeauftragten oder einem anderen für die Sicherheit zuständigem Mitglied des Managements übertragen?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?						
12.5.1	Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren;	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen	☐	☐	☐	☐	☐
12.5.2	Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das jeweilige Personal;	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen	☐	☐	☐	☐	☐
12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen	☐	☐	☐	☐	☐
12.5.4	Verwaltung von Benutzerkonten einschließlich Hinzufügen, Löschen und Ändern;	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen	☐	☐	☐	☐	☐
12.5.5	Überwachung und Kontrolle des gesamten Datenzugriffs;	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen	☐	☐	☐	☐	☐
12.6	(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheitheitsrichtlinien und Verfahren der Karteninhaberdaten zu vermitteln?	▪ Sicherheitsbewusstseinsprogramm durchgehen	☐	☐	☐	☐	☐
	(b) Umfassen die Verfahren des Sicherheitsbewusstseinsprogramms folgende Punkte?						
12.6.1	(a) Werden im Sicherheitsbewusstseinsprogramm mehrere Methoden zur Vermittlung des Bewusstseins für Sicherheitsprobleme angesprochen (beispielsweise Poster, Briefe, Memos, webbasierte Schulungen, Meetings und Sonderaktionen)? ***Hinweis:*** *Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechten auf Karteninhaberdaten.*	▪ Sicherheitsbewusstseinsprogramm durchgehen ▪ Verfahren des Sicherheitsbewusstseinsprogramms durchgehen ▪ Nachweise über die Teilnahme am Sicherheitsbewusstseinsprogramm überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Werden Mitarbeiterschulungen anlässlich von Neueinstellungen und anschließend mindestens einmal im Jahr durchgeführt?	▪ Verfahren und Dokumentation des Sicherheitsbewusstseinsprogramms untersuchen	☐	☐	☐	☐	☐
	(c) Haben die Mitarbeiter an entsprechenden Schulungen teilgenommen und sind sie sich darüber bewusst, wie wichtig die Sicherheit der Karteninhaberdaten ist?	▪ Mitarbeiter befragen	☐	☐	☐	☐	☐
12.6.2	Werden die Mitarbeiter mindestens einmal pro Jahr aufgefordert zu bestätigen, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben?	▪ Verfahren und Dokumentation des Sicherheitsbewusstseinsprogramms untersuchen	☐	☐	☐	☐	☐
12.7	Werden potenzielle Mitarbeiter (siehe Definition des Begriffs „Personal“ oben) vor der Einstellung eingehend geprüft, um das Risiko interner Angriffe so gering wie möglich zu halten? *Beispiele für Hintergrundinformationen sind frühere Tätigkeiten, eventuelle Vorstrafen, die finanzielle Situation und Referenzen bisheriger Arbeitgeber.* ***Hinweis:*** *Für potentielle neue Mitarbeiter wie z. B. Kassierer, die nie Zugriff auf mehrere Kartennummern gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.*	▪ Leitung der Personalabteilung befragen	☐	☐	☐	☐	☐
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert und gepflegt?						
12.8.1	Wird eine Liste von Dienstanbietern mit Angabe einer Beschreibung der geleisteten Dienstleistung gepflegt?	▪ Richtlinien und Verfahren durchgehen ▪ Prozesse überprüfen ▪ Liste der Dienstanbieter überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
12.8.2	Wird eine schriftliche Vereinbarung aufbewahrt, mit der bestätigt wird, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden bzw. die er für den Kunden speichert, verarbeitet oder überträgt, oder dass die Sicherheit der CDE betroffen sein könnte. ***Hinweis:*** *Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.*	▪ Schriftliche Vereinbarungen überprüfen ▪ Richtlinien und Verfahren durchgehen	☐	☐	☐	☐	☐
12.8.3	Gibt es ein eindeutiges Verfahren für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht?	▪ Prozesse überprüfen ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen	☐	☐	☐	☐	☐
12.8.4	Gibt es ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard?	▪ Prozesse überprüfen ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen	☐	☐	☐	☐	☐
12.8.5	Werden Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden, aufbewahrt?	▪ Prozesse überprüfen ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen	☐	☐	☐	☐	☐
12.9	*Diese Anforderung gilt nur für Dienstanbieter.*						
12.10	Wurde wie folgt ein Vorfallreaktionsplan implementiert, um umgehend auf mögliche Sicherheitsverletzungen im System zu reagieren?						
12.10.1	(a) Wurde ein Vorfallreaktionsplan erstellt, der im Falle einer Systemsicherheitsverletzung im System implementiert wird?	▪ Vorfallreaktionsplan überprüfen ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
	(b) Umfasst der Plan mindestens die folgenden Punkte?						
	• Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken;	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
	• konkrete Verfahren für die Reaktion auf Vorfälle;	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
	• Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs;	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
	• Verfahren zur Datensicherung;	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
	• Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen;	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
	• Abdeckung sämtlicher wichtigen Systemkomponenten;	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
	• Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle.	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
12.10.2	Wird der Plan mindestens jährlich, einschließlich aller in Anforderung 12.10.1 genannter Elemente, überprüft und getestet?	▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
12.10.3	Steht bestimmtes Personal rund um die Uhr zur Verfügung, um auf Alarme zu reagieren?	▪ Prozesse überprüfen ▪ Richtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.10.4	Werden die Mitarbeiter mit Verantwortung im Bereich der Sicherheitsverletzungs-Reaktion angemessen geschult?	▪ Prozesse überprüfen ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.10.5	Sind im Vorfallreaktionsplan Alarme der Sicherheitsüberwachungssysteme enthalten?	▪ Prozesse überprüfen ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen	☐	☐	☐	☐	☐
12.10.6	Wurde ein Prozess entwickelt und implementiert, um den Vorfallreaktionsplan je nach den gelernten Lektionen und Branchenentwicklungen zu ändern und zu aktualisieren?	▪ Prozesse überprüfen ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen ▪ Verantwortliche Mitarbeiter befragen	☐	☐	☐	☐	☐
12.11	*Diese Anforderung gilt nur für Dienstanbieter*						

Anhang A: Zusätzliche PCI DSS Anforderungen

Anhang A1: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsamem Hosting

Dieser Anhang wird nicht für Händlerbeurteilungen verwendet.

Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**	**Nicht geprüft**
A2.1	*Für POS POI -Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese Verbinden), die SSL und/oder eine frühe Version von TLS verwenden:* • Ist bestätigt, dass die Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind *Oder:* • Gibt es einen offiziellen Plan zur Risikoabschwächung und Migration gemäß Anforderung A2.2?	▪ Überprüfen Sie die Dokumentation (zum Beispiel Herstellerdokumente, Details der System-/Netzwerkkonfiguration, usw.), sie bestätigt, dass die POS POI -Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind	☐	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*				
			Ja	Ja, mit CCW	Nein	Nicht zutr.	Nicht geprüft
A2.2	Gibt es einen offiziellen Plan zur Risikoabschwächung und Migration für alle Implementierungen, die SSL und/oder eine frühe Version von TLS (anders als in A2.1 erlaubt) verwenden, der Folgendes umfasst: ▪ Beschreibung der Verwendung, einschließlich; Art der verarbeiteten Daten, Arten und Anzahl der Systeme, die SSL/eine frühe Version von TLS verwenden/unterstützen, Art der Umgebung; ▪ Ergebnisse der Risikobewertung und vorhandene Kontrollen zur Risikominderung; ▪ Beschreibung der Prozesse zur Überwachung neuer Schwachstellen in Zusammenhang mit SSL/einer frühen Version von TLS; ▪ Beschreibung der Verfahren zur Änderungskontrolle, die implementiert wurden, um zu gewährleisten, dass SSL/eine frühe Version von TLS nicht in neuen Umgebungen implementiert wird; ▪ Einen Überblick über den Migrationsprojektplan, einschließlich einem Termin für den Abschluss der Migration, nicht später als der 30. Juni 2018?	▪ Überprüfen Sie den dokumentierten Plan zur Risikoabschwächung und Migration	☐	☐	☐	☐	☐
A2.3	*Diese Anforderung gilt nur für Dienstanbieter*						

Anhang A3: Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation, DESV)

Dieser Anhang gilt ausschließlich für Einheiten, welche von einer Zahlungsmarke oder Acquirer zu einer zusätzlichen Überprüfung der vorhandenen PCI-DSS-Anforderungen festgelegt wurden. Einheiten, von welchen eine Überprüfung verlangt wird, müssen die DESV ergänzende Berichtsvorlage und die ergänzende Konformitätsbescheinigung für Berichterstattung verwenden, sowie sich an die entsprechende Zahlungsmarke bzw. Acquirer bezüglich der Einreichverfahren wenden.

Anhang B: Arbeitsblatt – Kompensationskontrollen

Bestimmen Sie anhand dieses Arbeitsblatts die Kompensationskontrollen für alle Anforderungen, bei denen „Ja, mit CCW" markiert wurde.

Hinweis: *Nur Unternehmen, die eine Risikoanalyse vorgenommen und legitime technologische oder dokumentierte geschäftliche Hindernisse nachweisen können, können den Einsatz von Kompensationskontrollen zu Konformitätszwecken in Erwägung ziehen.*

Informationen zu Kompensationskontrollen sowie Hinweise zum Ausfüllen dieses Arbeitsblatts finden Sie in den PCI-DSS-Anhängen B, C und D.

Anforderungsnummer und -definition:

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	
2. Ziel	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

Anhang C: Erläuterung der Nichtanwendbarkeit

Falls die Spalte „N/A“ (Nicht zutreffend) im Fragebogen markiert wurde, erläutern Sie bitte im Arbeitsblatt, warum die zugehörige Anforderung nicht für Ihr Unternehmen gilt.

Anforderung	Grund, warum die Anforderung nicht anwendbar ist.
Beispiel:	
3.4	Karteninhaberdaten werden nie in elektronischer Form aufbewahrt.

Anhang D: Erklärung zu nicht geprüften Anforderungen

Falls die Spalte „Nicht geprüft“ in diesem Fragebogen markiert wurde, erklären Sie auf diesem Arbeitsblatt, warum die betreffende Anforderung nicht im Rahmen der Beurteilung geprüft wurde.

Anforderung	Beschreiben Sie, welche Teile der Anforderung nicht geprüft wurden.	Begründen Sie, warum die Anforderungen nicht geprüft wurden.
Beispiele:		
Anforderung 12	*Nur Anforderung 12.2 wurde geprüft. Alle anderen Anforderungen unter Anforderung 12 wurden von der Prüfung ausgeschlossen.*	*Diese Beurteilung umfasst ausschließlich Anforderungen unter Meilenstein 1 des bevorzugten Verfahrens.*
Anforderungen 1 bis 8 sowie 10 bis 12	*Nur Anforderung 9 wurde im Rahmen dieser Beurteilung geprüft. Alle anderen Anforderungen wurden von der Prüfung ausgeschlossen.*	*Das Unternehmen ist ein physischer Hostinganbieter (CO-LO), und bei dieser Beurteilung wurden ausschließlich physische Sicherheitskontrollen berücksichtigt.*

3. Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

Diese Konformitätsbescheinigung basiert auf den Ergebnissen, welche im SBF D (Abschnitt 2) mit Datum vom *(Abschlussdatum des SBF) notiert wurden.*

Aufgrund der Ergebnisse des SBF D vom (Abschlussdatum) stellen die in Teil 3b bis 3d angegebenen Unterzeichner den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (Datum) benannte Stelle fest: (***Zutreffendes ankreuzen):***

☐	**Konform:** Alle Abschnitte des PCI DSS SBF sind vollständig und alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung **KONFORM**. *(Name des Händlerunternehmens)* hat somit vollständig Konformität mit dem PCI DSS gezeigt.
☐	**Nicht konform:** Nicht alle Abschnitte des PCI DSS SBF sind vollständig und/oder nicht alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung **NICHT KONFORM**. *(Name des Händlerunternehmens)* hat somit nicht vollständige Konformität mit dem PCI DSS gezeigt. **Zieldatum** für Konformität: Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen.*
☐	**Konform, jedoch mit gesetzlicher Ausnahme:** Eine oder mehrere Anforderungen sind aufgrund einer gesetzlichen Einschränkung, die das Erfüllen der jeweiligen Anforderung(en) unmöglich macht, mit „Nein“ gekennzeichnet. Bei dieser Option ist eine zusätzliche Prüfung durch den Acquirer oder die Zahlungsmarke erforderlich. *Falls diese Option markiert ist, arbeiten Sie folgende Punkte ab:*

Betroffene Anforderung	Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern

Teil 3a. Feststellung des Status

Unterzeichner bestätigt:

(Zutreffendes ankreuzen)

☐	Der PCI-DSS-Selbstbeurteilungsfragebogen D, Version *(Version des SBF)*, wurde den enthaltenen Anleitungen gemäß ausgefüllt.
☐	Alle Informationen im oben genannten SBF und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung in allen materiellen Aspekten korrekt dar.
☐	Mein Zahlungsanwendungsanbieter hat mir bestätigt, dass in meinem Zahlungssystem nach der Autorisierung keine empfindlichen Authentifizierungsdaten gespeichert werden.
☐	Ich habe den PCI DSS gelesen und erkenne an, dass ich jederzeit die für meine Umgebung geltende PCI-DSS-Konformität aufrechterhalten muss.
☐	Für den Fall, dass sich meine Umgebung ändert, erkenne ich an, dass ich meine Umgebung erneut beurteilen und etwaige zusätzliche PCI-DSS-Anforderungen erfüllen muss.

Teil 3a. Feststellung des Status (Fortsetzung)	
☐	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung vollständige Spurdaten („Full-Track-Daten“)[1], CAV2-, CVC2-, CID-, CVV2[2]- oder PIN-Daten[3] gespeichert wurden.
☐	ASV-Scans werden vom PCI SSC Approved Scanning Vendor *(Name des ASV) durchgeführt.*

Teil 3b. Bescheinigung des Händlers	
Unterschrift des Beauftragten des Händlers ↗	*Datum:*
Name des Beauftragten des Händlers:	*Titel:*

Teil 3c. Bestätigung durch den QSA (Qualified Security Assessor) (sofern zutreffend)	
Falls ein QSA an dieser Beurteilung beteiligt war, beschreiben Sie bitte dessen Aufgabe:	

Unterschrift des ordnungsgemäß ermächtigten Vertreters des QSA Unternehmens ↗	*Datum:*
Name des ordnungsgemäß ermächtigten Vertreters:	*Unternehmen des QSA:*

Teil 3d. Beteiligung eines ISA (Internal Security Assessor) (sofern zutreffend)	
Falls ein ISA an dieser Beurteilung beteiligt war oder dabei geholfen hat, identifizieren Sie bitte den ISA-Mitarbeiter und beschreiben Sie dessen Aufgabe:	

[1] Im Magnetstreifen verschlüsselte Daten oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Spurdaten speichern. Die einzigen Spurdatenelemente, die aufbewahrt werden dürfen, sind die primäre Kontonummer (PAN), das Ablaufdatum und der Name des Karteninhabers.

[2] Der drei- oder vierstellige Wert, der neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

[3] Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht

Teil 4. Aktionsplan für Status „Nicht konform“

Wählen Sie zu jeder Anforderung die zutreffende Antwort auf die Frage nach der Konformität mit PCI-DSS-Anforderungen aus. Wenn Sie einen der Punkte mit „Nein“ beantworten, müssen Sie möglicherweise das Datum angeben, an dem das Unternehmen die Anforderung voraussichtlich erfüllen wird. Geben Sie außerdem eine kurze Beschreibung der Maßnahmen an, die zur Erfüllung der Anforderung ergriffen werden.

Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen.

PCI-DSS-Anforderung	Anforderungsbeschreibung	Konform mit PCI-DSS-Anforderungen (zutreffende Antwort auswählen)		Datum bis zur Mängelbeseitigung und Abhilfemaßnahmen (falls „Nein“ ausgewählt wurde)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	☐	☐	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	☐	☐	
3	Schutz gespeicherter Karteninhaberdaten	☐	☐	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	☐	☐	
5	Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen	☐	☐	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	☐	☐	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	☐	☐	
8	Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten	☐	☐	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	☐	☐	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	☐	☐	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	☐	☐	
12	Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.	☐	☐	

Anhang A2	Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden	☐	☐