Zahlungskartenbranche (PCI)
Datensicherheitsstandard
Selbstbeurteilungsfragebogen A-EP und Konformitätsbescheinigung

Teilweise externe E-Commerce-Händler, die eine Dritt-Website zur Zahlungsabwicklung nutzen

Zur Verwendung mit PCI DSS Version 3.2.1

Revision 1.0
Juni 2018

Dokumentänderungen

Datum	PCI DSS Version	SBF Revision	Beschreibung
Nicht zutr.	1.0		(findet keine Anwendung)
Nicht zutr.	2.0		(findet keine Anwendung)
Februar 2014	3.0		Der neue SBF wurde zur Erfüllung von Anforderungen in Bezug auf E-Commerce-Händler mit einer Website entwickelt, auf der selbst keine Karteninhaberdaten eingehen, die jedoch die Sicherheit der Zahlungstransaktion und/oder die Integrität der Seite beeinflusst, von der die Karteninhaberdaten akzeptiert werden. Anpassung der Inhalte an die Anforderungen und Prüfverfahren gemäß PCI DSS v3.0.
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*.
Juni 2015	3.1		Anforderung 11.3 zur Fehlerbehebung aktualisiert.
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 zur Übereinstimmung mit 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.* Anforderungen von PCI DSS v3.2 hinzugefügt Anforderungen 1, 5, 6, 7, 8, 10, 11 und Anhang A2.
Januar 2017	3.2	1.1	Dokumentänderungen wurden aktualisiert, um die in der Aktualisierung von April 2016 hinzugefügten Anforderungen zu verdeutlichen.
Juni 2018	3.2.1	1.0	Aktualisiert zur Übereinstimmung mit PCI DSS v3.2.1. Ausführliche Informationen zu den Änderungen am PCI DSS finden Sie unter *PCI DSS – Änderungsübersicht von PCI DSS Version 3.2 auf 3.2.1.*

DANKSAGUNG:

Die englische Textversion dieses Dokuments wie auf der PCI SSC-Website angezeigt gilt für alle Zwecke als offizielle Version dieses Dokuments. Für den Fall von Mehrdeutigkeit oder Unstimmigkeit zwischen diesem und dem englischen Text hat die englische Version Vorrang.

Inhalt

Vorbereitung

SBF A-EP wurde entwickelt zur Erfüllung von Anforderungen in Bezug auf E-Commerce-Händler mit einer Website, auf der selbst keine Karteninhaberdaten eingehen, die jedoch die Sicherheit der Zahlungstransaktion und/oder die Integrität der Seite beeinflusst, von der die Karteninhaberdaten akzeptiert werden.

SBF A-EP-Händler sind E-Commerce-Händler, die ihren E-Commerce-Zahlungskanal teilweise an nach PCI DSS validierte Dritte ausgliedern und Karteninhaberdaten nicht elektronisch auf ihren Systemen oder an ihren Standorten speichern, verarbeiten oder übertragen.

SBF A-EP-Händler bestätigen im Zusammenhang mit diesem Zahlungskanal folgende Bedingungen:

- Ihr Unternehmen akzeptiert ausschließlich E-Commerce-Transaktionen;
- Die Verarbeitung von Karteninhaberdaten, mit Ausnahme der Zahlungsseite, wird vollständig an eine nach PCI DSS validierte externe Abrechnungsstelle vergeben;
- Ihre E-Commerce-Website empfängt keine Karteninhaberdaten, steuert jedoch die Umleitung von Verbrauchern oder deren Karteninhaberdaten an eine nach PCI DSS validierte externe Abrechnungsstelle;
- Falls die Website des Händlers von einem Drittanbieter gehostet wird, ist dieser Anbieter nach allen geltenden Anforderungen gemäß PCI DSS validiert (u. a. einschließlich PCI DSS Appendix A, falls es sich um einen gemeinsam genutzten Hosting-Anbieter handelt);
- Sämtliche Elemente der Zahlungsseiten, die an den Browser des Verbrauchers übermittelt werden, stammen entweder von der Website des Händlers oder von einem PCI-DSS-konformen Serviceanbieter;
- Ihr Unternehmen speichert, verarbeitet oder überträgt Karteninhaberdaten weder vor Ort noch auf Ihren Systemen in elektronischer Form, sondern verlässt sich voll und ganz auf einen oder mehrere Drittunternehmen, die diese Funktionen übernehmen;
- Ihr Unternehmen hat bestätigt, dass die Speicherung, Verarbeitung und/oder Übertragung der Karteninhaberdaten durch das oder die Drittunternehmen PCI-DSS-konform sind; und
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, sind in Papierform (zum Beispiel Papierdokumente und -quittungen), und diese Dokumente werden nicht elektronisch entgegengenommen.

dieser SBF gilt ausschließlich für E-Commerce-Kanäle.

Diese verkürzte Version des SBF enthält Fragen, die für eine bestimmte Art von Umgebungen kleiner Handelsunternehmen, so wie in den Qualifikationskriterien oben definiert, gelten. Sollten für Ihre Umgebung PCI-DSS-Anforderungen gelten, die nicht in diesem SBF behandelt werden, kann dies ein Hinweis darauf sein, dass dieser SBF nicht für Ihr Unternehmen geeignet ist. Zusätzlich müssen Sie auch weiterhin alle geltenden PCI-DSS-Anforderungen erfüllen, um als PCI-DSS-konform angesehen zu werden.

Hinweis: *Im Sinne dieses SBF gelten alle PCI-DSS-Anforderungen, die sich auf die "Karteninhaberdaten-Umgebung" beziehen, für die Webseite(n) des Händlers. Dies beruht darauf, dass die Webseite des Händlers direkt beeinflusst, wie Karteninhaberdaten übertragen werden, selbst wenn die Webseite selbst keine Karteninhaberdatenen empfängt.*

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 (gemäß Definition in Teil 2g der Konformitätsbescheinigung).
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 A-EP)
   - 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, dem Kartenunternehmen oder 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
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 „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.

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

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.

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 an Ihren Acquirer (Handelsbank) oder die Kartenunternehmen, um Berichts- und Sendeverfahren zu bestimmen.

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 Ihr Kartenunternehmen.*

Teil 2. Zusammenfassung für die Geschäftsleitung *(Fortsetzung)*

Teil 2b. Beschreibung des Zahlungskartengeschäfts

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

Teil 2c. Standorte

Listen Sie alle Einrichtungen (beispielsweise Einzelhandelsgeschäfte, Büroräume, Rechenzentren, Callcenter usw.) sowie eine Zusammenfassung der Standorte auf, die in der PCI-DSS-Prüfung berücksichtigt wurden.

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

Teil 2d. Zahlungsanwendungen

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	Versions-nummer	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 2. Zusammenfassung für die Geschäftsleitung *(Fortsetzung)*

Teil 2f. Externe Dienstanbieter

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

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

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

Teil 2g. Qualifikation zum Ausfüllen des SBF A-EP

Der Händler bestätigt die Qualifikation zum Ausfüllen dieser Kurzfassung des Selbstbeurteilungsfragebogens (in Bezug auf diesen Zahlungskanal) aus folgenden Gründen:

☐	Händler akzeptiert nur E-Commerce-Transaktionen;
☐	Die Verarbeitung von Karteninhaberdaten, mit Ausnahme der Zahlungsseite, wird vollständig an eine nach PCI DSS validierte externe Abrechnungsstelle vergeben;
☐	Die E-Commerce-Website des Händlers empfängt keine Karteninhaberdaten, steuert jedoch die Umleitung von Verbrauchern oder deren Karteninhaberdaten an eine nach PCI DSS validierte externe Abrechnungsstelle;
☐	Falls die Website des Händlers von einem Drittanbieter gehostet wird, ist dieser Anbieter nach allen geltenden Anforderungen gemäß PCI DSS validiert (u. a. einschließlich PCI DSS Appendix A, falls es sich um einen gemeinsam genutzten Hosting-Anbieter handelt);

☐	Sämtliche Elemente der Zahlungsseiten, die an den Browser des Verbrauchers übermittelt werden, stammen entweder von der Website des Händlers oder von einem PCI-DSS-konformen Serviceanbieter;
☐	Der Händler speichert, verarbeitet oder überträgt keine Karteninhaberdaten in elektronischer Form, weder vor Ort noch auf seinen Systemen, sondern verlässt sich voll und ganz auf einen oder mehrere Dritte, der/die diese Funktionen übernimmt/übernehmen;
☐	Der Händler hat bestätigt, dass die Speicherung, Verarbeitung und/oder Übertragung der Karteninhaberdaten durch das oder die Drittunternehmen PCI-DSS-konform sind; **und**
☐	Der Händler bewahrt ausschließlich Papierdokumente oder -quittungen mit Karteninhaberdaten auf und diese Dokumente werden nicht elektronisch empfangen.

2. Abschnitt: Selbstbeurteilungsfragebogen A-EP

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 eines sicheren Netzwerks

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.
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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(b) Entspricht das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration?	▪ Standards der Firewall-Konfiguration mit dem aktuellen Netzwerkdiagramm vergleichen.	☐	☐	☐	☐
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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
1.3.7	(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);* • *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 (oder eine gleichwertige Funktion) auf allen mobilen Geräten (einschließlich betriebseigener Geräte bzw. Geräte der Mitarbeiter) 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 CDE eingesetzt werden?	▪ Richtlinien und Konfigurationsstandards überprüfen. ▪ Mobile und/oder mitarbeitereigene Geräte untersuchen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(b) Ist die persönliche Firewall-Software (oder eine gleichwertige Funktion) 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.
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(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.	☐	☐	☐	☐
2.2	(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.
2.2 *(Forts.)*	(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.
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?	▪ 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.
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?					
	(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.	☐	☐	☐	☐

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.
3.2	(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 ein, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern (auch wenn diese verschlüsselt sind)?					
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	☐	☐	☐	☐

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.**
4.1	(a) Werden eine starke Kryptographie und Sicherheitsprotokolle eingesetzt, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen? ***Hinweis:*** *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.	☐	☐	☐	☐
	(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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
4.2	(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 Schwachstellen-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.
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. ▪ Antivirus-Konfigurationen einschließlich der Master-Installation untersuchen. ▪ Systemkomponenten untersuchen.	☐	☐	☐	☐
	(b) Sind automatische Updates und regelmäßige Scans aktiviert und werden sie regelmäßig durchgeführt?	▪ Antivirus-Konfigurationen einschließlich der Master-Installation untersuchen. ▪ Systemkomponenten untersuchen.	☐	☐	☐	☐
	(c) Generieren alle Virenschutzmechanismen Prüfprotokolle und werden die Protokolle gemäß PCI-DSS-Anforderung 10.7 aufbewahrt?	▪ Antivirus-Konfigurationen untersuchen. ▪ Prozesse zur Aufbewahrung von Protokollen durchgehen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
5.3	Aspekte bei Antivirenmechanismen: ▪ Werden alle Antivirenmechanismen aktiv ausgeführt? ▪ Sind sie gegen benutzerseitige Deaktivierungen oder Veränderungen gesichert? ***Hinweis:*** *Antivirenlösungen dürfen nur dann vorübergehend deaktiviert werden, wenn es einen triftigen technischen Grund dafür gibt. Hierzu ist für jeden Einzelfall die Genehmigung der Geschäftsführung einzuholen. Wenn der Virenschutz aus bestimmten Gründen deaktiviert werden muss, ist hierfür eine förmliche Autorisierung erforderlich. Möglicherweise sind außerdem für den Zeitraum, in dem der Virenschutz nicht aktiv ist, zusätzliche Sicherheitsmaßnahmen zu treffen.*	▪ Antivirus-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.
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.
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.	☐	☐	☐	☐
6.4.5	(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?					
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) Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt	▪ 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.
	(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.	☐	☐	☐	☐
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?	▪ Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle. ▪ Durchsicht der Dokumentation zur Änderungskontrolle. ▪ Mitarbeiter befragen. ▪ Beobachten betroffener Systeme oder Netzwerke.	☐	☐	☐	☐
6.5	Wird in Softwareentwicklungsprozessen auf häufige Sicherheitsrisiken bei der Programmierung eingegangen?	▪ Richtlinien und Verfahren zur Softwareentwicklung überprüfen.	☐	☐	☐	☐
	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?					
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
6.5.2	Zielen die Codierungsverfahren auf die Vermeidung von Pufferüberläufen ab?	▪ 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.	☐	☐	☐	☐
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.
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, der 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.
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.
7.1	Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten wie folgt ausschließlich auf jene Personen beschränkt, deren Tätigkeit diesen Zugriff erfordert?					
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	▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen. ▪ Mitarbeiter befragen. ▪ Management befragen. ▪ Privilegierte Benutzer-IDs überprüfen.	☐	☐	☐	☐
7.1.3	Werden Zugriffsberechtigungen anhand der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter zugewiesen?	▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen. ▪ 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.	☐	☐	☐	☐

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.**
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.	☐	☐	☐	☐
	(b) Werden die Remote-Zugriff-Konten von Dritten während der Nutzung überwacht?	▪ Mitarbeiter befragen. ▪ Prozesse überprüfen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
8.1.6	(a) Werden wiederholte Zugriffsversuche begrenzt, indem die Benutzer-ID nach mehr als sechs Versuchen gesperrt wird?	▪ Kennwortverfahren überprüfen. ▪ Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐
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) Unterliegt die nicht entschlüsselbare Übertragung und Speicherung von Kennwörtern/Kennsätzen auf sämtlichen Systemkomponenten einer sicheren Verschlüsselung?	▪ Kennwortverfahren überprüfen. ▪ Anbieterdokumentation durchgehen. ▪ Systemkonfigurationseinstellungen untersuchen. ▪ Kennwortdateien überprüfen. ▪ Datenübertragungen überprüfen.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
8.2.4	(a) Werden Benutzerkennwörter/-sätze mindestens einmal alle 90 Tage geändert?	▪ Kennwortverfahren überprüfen. ▪ Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐
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.	☐	☐	☐	☐
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.*					

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
8.3.1	Ist die Multi-Faktor-Authentifizierung fester Bestandteil für alle Nichtkonsolen-Zugriffe auf das CDE durch Mitarbeiter mit Verwaltungszugriff?	▪ 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.	☐	☐	☐	☐
	(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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
8.6	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.	☐	☐	☐	☐
8.8	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.
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.	☐	☐	☐	☐
9.5	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.	☐	☐	☐	☐
9.6	(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.	☐	☐	☐	☐
9.8	(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.	☐	☐	☐	☐
	(c) Erfolgt die Vernichtung von Medien wie nachstehend beschrieben?					

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
9.8.1	(a) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen. ▪ Mitarbeiter befragen. ▪ Prozesse überprüfen.	☐	☐	☐	☐
	(b) Werden Container zur Aufbewahrung von zu vernichtenden Informationen so geschützt, dass Zugriffe auf diese Inhalte vermieden werden?	▪ Sicherheit von Containern überprüfen.	☐	☐	☐	☐

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.
10.1	Sind Audit-Trails für die Systemkomponenten vorhanden und aktiv?	▪ Prozesse überprüfen. ▪ Systemadministrator befragen.	☐	☐	☐	☐
	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?					
10.2.2	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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
	(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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(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	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.*					
10.6.1	(b) Werden die folgenden Protokolle und Sicherheitsereignisse mindestens täglich manuell oder mittels Protokolltools überprüft? – 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. ▪ Prozesse überprüfen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐
10.6.2	(b) Werden Protokolle aller weiteren Systemkomponenten regelmäßig – manuell oder mittels Protokolltools – anhand der Richtlinien und Risikomanagementstrategie des Unternehmens überprüft?	▪ Sicherheitsrichtlinien und -verfahren durchgehen. ▪ Dokumentation zur Risikobeurteilung durchgehen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
10.6.3	(b) Werden die bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten nachverfolgt?	▪ Sicherheitsrichtlinien und -verfahren durchgehen. ▪ Prozesse überprüfen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐
10.7	(b) Werden Prüfprotokolle mindestens ein Jahr aufbewahrt?	▪ Sicherheitsrichtlinien und -verfahren durchgehen. ▪ Mitarbeiter befragen. ▪ Prüfprotokolle überprüfen.	☐	☐	☐	☐
	(c) Sind die Protokolle zu Analysezwecken mindestens drei Monate lang unmittelbar verfügbar?	▪ Mitarbeiter befragen. ▪ Prozesse überprüfen.	☐	☐	☐	☐

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.
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(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.	☐	☐	☐	☐
	(b) Sieht der Scanprozess erneute Scans vor, bis … – … bei externen Scans keine Sicherheitsrisiken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung von 4.0 oder höher 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.
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.
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 verwendeten 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.	☐	☐	☐	☐
	(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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
11.5 *(Forts.)*	(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.	☐	☐	☐	☐
11.5.1	Wurde ein Prozess implementiert, um auf Alarme der Änderungserkennungslösung reagieren zu können?	▪ Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐

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.
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.	☐	☐	☐	☐
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen. ▪ Per Stichprobe zuständige Mitarbeiter befragen.	☐	☐	☐	☐
12.5	(b) Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?					
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.	☐	☐	☐	☐
12.6	(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheitheitsrichtlinien und Verfahren der Karteninhaberdaten zu vermitteln?	▪ Sicherheitsbewusstseinsprogramm durchgehen.	☐	☐	☐	☐
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?					

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
12.8.1	Wird eine Liste von Dienstanbietern mit Angabe einer Beschreibung der geleisteten Dienstleistung(en) gepflegt?	▪ Richtlinien und Verfahren durchgehen. ▪ Prozesse überprüfen. ▪ Liste der Dienstanbieter überprüfen.	☐	☐	☐	☐
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.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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.	☐	☐	☐	☐
	(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.	☐	☐	☐	☐

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, die SSL/frühe Versionen von TLS in POS-POI-Terminalverbindungen mit vorliegender Karte verwenden

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
A2.1	*Für POS-POI-Terminals (**beim Händler oder Zahlungsannahmeort**), die SSL und/oder frühe Versionen von TLS verwenden:* Ist bestätigt, dass die Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind? ***Hinweis:** Diese Anforderung soll für die Einheit mit dem POS-POI-Terminal, wie z. B. den Händler, gelten. Diese Anforderung richtet sich nicht an Dienstanbieter, die als Abschluss- oder Verbindungspunkt für diese POS-POI-Terminals dienen. Die Anforderungen A2.2 und A2.3 gelten für POS-POI-Dienstanbieter.*	▪ Dokumentation dahingehend überprüfen (beispielsweise Anbieterdokumentation, Details der System-/Netzwerkkonfiguration usw.), dass die POS POI-Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind.	☐	☐	☐	☐

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

Dieser Anhang gilt ausschließlich für Einheiten, welche von einem Kartenunternehmen oder Acquirer zu einer zusätzlichen Überprüfung der vorhandenen PCI-DSS-Anforderungen aufgefordert wurden. Einheiten, von denen eine Überprüfung verlangt wird, müssen die ergänzende DESV-Berichtsvorlage und die ergänzende Konformitätsbescheinigung für Berichterstattung verwenden, sowie sich an das entsprechende Kartenunternehmen 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 Kompensations-kontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. Validierung der Kompensations-kontrollen	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.

3. Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

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

Auf der Grundlage der Ergebnisse des SBF A-EP vom (Abschlussdatum) stellen die in Teil 3b bis 3d angegebenen Unterzeichner den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (Datum) ermittelte 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 Ihrem/Ihren Kartenunternehmen 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 das Kartenunternehmen 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 A-EP, 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 Ihrem/Ihren Kartenunternehmen 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	Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter	☐	☐	
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 Antivirussoftware und Programmen.	☐	☐	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	☐	☐	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf	☐	☐	
8	Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten.	☐	☐	
9	Beschränkung des physischen Zugriffs auf Karteninhaberdaten	☐	☐	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	☐	☐	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	☐	☐	
12	Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal	☐	☐	

Anhang A2	Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/frühe Versionen von TLS in POS-POI-Terminalverbindungen mit vorliegender Karte verwenden.	☐	☐	

** Die hier angegebenen PCI-DSS-Anforderungen beziehen sich auf die Fragen in Abschnitt 2 des SBF.*