



Payment Card Industry (PCI)
Datensicherheitsstandard
**Selbstbeurteilungsfragebogen C
und Konformitätsbescheinigung**

**Händler mit
Zahlungssystemen, die mit
dem Internet verbunden sind –
kein elektronischer Karteninhaberdaten-
Speicher**

Zur Verwendung mit PCI DSS Version 3.2

Revision 1.1
Januar 2017

Dokumentänderungen

Datum	PCI DSS Version	SBF Revision	Beschreibung
Oktober 2008	1.2		Anpassung der Inhalte an den neuen PCI DSS v1.2 und Implementieren kleinerer Änderungen nach der Ursprungsversion v1.1.
Oktober 2010	2.0		Anpassung der Inhalte an die neuen Anforderungen und Testverfahren nach PCI DSS v2.0.
Februar 2014	3.0		Anpassung der Inhalte an die Anforderungen und Testverfahren nach PCI DSS v3.0 sowie Integration weiterer Reaktionsmöglichkeiten.
April 2015	3.1		Aktualisiert im Sinne des PCI-DSS v3.1. Ausführliche Informationen finden Sie unter <i>PA-DSS – Änderungsübersicht von PA-DSS Version 3.0 auf 3.1</i> .
Juli 2015	3.1	1.1	Aktualisiert durch Entfernen von Bezügen auf „bewährte Verfahren“ vor dem 30. Juni 2015.
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 <i>PCI DSS – Änderungsübersicht von PCI DSS Version 3.1 auf 3.2</i> . Anforderungen von PCI DSS v3.2 hinzugefügt Anforderungen 8, 9 und Anhang A2.
Januar 2017	3.2	1.1	Dokumentänderungen wurden aktualisiert, um die in der Aktualisierung von April 2016 hinzugefügten Anforderungen zu verdeutlichen. Es wurde eine Fußnote zum Abschnitt „Vorbereitung“ hinzugefügt, um den Zweck der zulässigen Systeme zu verdeutlichen. Die Kontrollkästchen in den Anforderungen 8.1.6 und 11.3.4 wurden angepasst.

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

Dokumentänderungen	i
Vorbereitung	iv
PCI-DSS-Selbstbeurteilung – Schritte zum Ausfüllen	iv
Erklärungen zum Selbstbeurteilungsfragebogen	v
<i>Erwartete Tests</i>	<i>v</i>
Ausfüllen des Selbstbeurteilungsfragebogens	vi
Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen	vi
Gesetzliche Ausnahme	vi
1. Abschnitt: Informationen zur Beurteilung	1
2. Abschnitt: Selbstbeurteilungsfragebogen C	4
Erstellung und Wartung sicherer Netzwerke und Systeme	4
<i>Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</i>	<i>4</i>
<i>Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden</i>	<i>6</i>
Schutz von Karteninhaberdaten	12
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i>	<i>12</i>
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i>	<i>14</i>
Unterhaltung eines Anfälligkeits-Managementprogramms	16
<i>Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen</i>	<i>16</i>
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen</i>	<i>18</i>
Implementierung starker Zugriffskontrollmaßnahmen	20
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf</i>	<i>20</i>
<i>Anforderung 8: Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten</i>	<i>21</i>
<i>Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken</i>	<i>25</i>
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken	30
<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten</i>	<i>30</i>
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse</i>	<i>33</i>
Befolgung einer Informationssicherheitsrichtlinie	39
<i>Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal</i>	<i>39</i>
Anhang A: Zusätzliche PCI DSS Anforderungen	43
<i>Anhang A1: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsamem Hosting</i>	<i>43</i>
<i>Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden</i>	<i>43</i>

Anhang A3:	<i>Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation, DESV)</i>	<i>44</i>
Anhang B:	Arbeitsblatt – Kompensationskontrollen	45
Anhang C:	Erläuterung der Nichtanwendbarkeit.....	46
3. Abschnitt:	Validierungs- und Bescheinigungsdetails	47

Vorbereitung

SBF C wurde speziell für die Anforderungen entwickelt, die für Händler gelten, deren Zahlungsanwendungssysteme (z. B. Point-Of-Sale-Systeme) mit dem Internet verbunden sind (z. B. über DSL oder Kabelmodem)

SAQ C Händler verarbeiten Karteninhaberdaten über POS-Systeme oder andere Zahlungsanwendungssysteme, die mit dem Internet verbunden sind und keine Karteninhaberdaten auf Computersystemen speichern. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder Versandhändler (Karte liegt nicht vor) handeln.

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

- Ihr Unternehmen verfügt über ein Zahlungsanwendungssystem und eine Internetverbindung auf demselben Gerät und/oder demselben Local Area Network (LAN);
- Das Zahlungsanwendungssystem/Internetgerät ist nicht mit anderen Systemen Ihrer Umgebung verbunden (dies kann mithilfe einer Netzwerksegmentierung zur Isolierung des Zahlungsanwendungssystems/Internetgeräts von allen anderen Systemen erreicht werden)¹;
- der physische Standort der POS-Umgebung ist nicht mit anderen Stellen oder Standorten verbunden, und jedes LAN ist nur für einen einzigen Standort eingerichtet;
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, sind in Papierform (zum Beispiel Papierdokumente und -quittungen), und diese Dokumente werden nicht elektronisch entgegengenommen; **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

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.

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 Dieses Kriterium zielt nicht darauf ab, mehr als einen der zugelassenen Systemtypen (d. h., ein Zahlungsanwendungssystem), die sich in derselben Netzwerkzone befinden, zu verbieten, solange die zugelassenen Systeme von anderen Arten von Systemen isoliert sind (z. B. durch die Implementierung der Netzwerksegmentierung). Darüber hinaus zielt dieses Kriterium nicht darauf ab, die definierten Systemarten daran zu hindern, Transaktionsinformationen über ein Netzwerk an Dritte zur Verarbeitung zu übertragen, wie an einen Acquirer oder Zahlungsabwickler.

- 1. Abschnitt (Teil 1 und 2 der Konformitätsbescheinigung) – Informationen zur Beurteilung und Executive Summary.
 - 2. Abschnitt – PCI-DSS-Selbstbeurteilungsfragebogen (SBF C)
 - 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 Selbstbeurteilungsfragebogens zur Verfügung. Ein Teil dieser Ressourcen ist unten aufgeführt:

Dokument	enthält:
PCI DSS <i>(Anforderungen und Sicherheitsbeurteilungsverfahren des PCI-Datensicherheitsstandards)</i>	<ul style="list-style-type: none"> • Leitfaden zum Umfang/Geltungsbereich • Leitfaden zum Zweck der PCI-DSS-Anforderungen • Detaillierte Informationen zu Testverfahren • Leitfaden zu Kompensationskontrollen
Anleitung und Richtlinien zum SBF	<ul style="list-style-type: none"> • Informationen zu allen SBF und ihren Qualifikationskriterien • Bestimmung des passenden SBF für Ihr Unternehmen
<i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>	<ul style="list-style-type: none"> • Beschreibungen und Definitionen von Begriffen, die im PCI DSS und in den Selbstbeurteilungsfragebögen vorkommen

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

Erwartete Tests

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

Ausfüllen des Selbstbeurteilungsfragebogens

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

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

Antwort	Wann trifft diese Antwort zu?
Ja	Die erwarteten Tests wurden durchgeführt und alle Elemente der Anforderung wurden wie angegeben erfüllt.
Ja, mit CCW (Compensating Control Worksheet, Arbeitsblatt zu Kompensationskontrollen)	Die erwarteten Tests wurden durchgeführt, und die Anforderung wurde unter Zuhilfenahme einer Kompensationskontrolle erfüllt. Für alle Antworten in dieser Spalte ist ein Arbeitsblatt zu Kompensationskontrollen (Compensating Control Worksheet, CCW) in Anhang B des SBF auszufüllen. Informationen zu Kompensationskontrollen und Hinweise zum Ausfüllen des Arbeitsblatts sind im PCI DSS enthalten.
Nein	Einige oder alle Elemente der Anforderung wurden nicht erfüllt, werden gerade implementiert oder müssen weiteren Tests unterzogen werden, ehe bekannt ist, ob sie vorhanden sind.
Nicht zutr. (Nicht zutreffend)	Die Anforderung gilt nicht für die Umgebung des Unternehmens. (Beispiele sind im <i>Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen</i> 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

Während viele Unternehmen, die SBF C ausfüllen, die Konformität mit allen PCI-DSS-Anforderungen bestätigen müssen, werden einige Unternehmen mit sehr spezifischen Geschäftsmodellen eventuell feststellen, dass einige Anforderungen für sie nicht gelten.

Ein Unternehmen, das z. B. überhaupt keine drahtlose Technologie verwendet, muss die Konformität mit den Abschnitten des PCI DSS, die sich speziell auf die Verwaltung drahtloser Technologien beziehen, nicht validieren (etwa die Anforderungen 1.2.3, 2.1.1 und 4.1.1). Bitte beachten Sie, dass Anforderung 11.1 (Verwendung eines Prozesses zur Erkennung unbefugter WLAN-Zugriffspunkte) auch beantwortet werden muss, wenn Sie in Ihrem Netzwerk keine drahtlose Technologie verwenden, weil der Prozess alle sicherheitsgefährdenden oder unerlaubten Geräte erfasst, die vielleicht ohne Ihr Wissen angeschlossen wurden.

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 bezüglich des ordnungsgemäßen Berichts- und Einreichungsverfahrens an den Acquirer (Handelsbank) oder die Zahlungsmarken.

Teil 1. Informationen zum Qualified Security Assessor und Händler

Teil 1a. Händlerinformationen

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

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

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

Teil 2. Zusammenfassung für die Geschäftsleitung

Teil 2a. Handelstätigkeit (alle zutreffenden Optionen auswählen)

<input type="checkbox"/> Einzelhändler	<input type="checkbox"/> Telekommunikation	<input type="checkbox"/> Lebensmitteleinzelhandel und Supermärkte
<input type="checkbox"/> Erdöl/Erdgas	<input type="checkbox"/> E-Commerce	<input type="checkbox"/> Schriftliche/Telefonische Bestellung (MOTO)
<input type="checkbox"/> Sonstiges (bitte angeben):		
Welche Arten von Zahlungskanälen werden von Ihrem Unternehmen bedient?	Welche Zahlungskanäle sind durch diesen SBF abgedeckt?	
<input type="checkbox"/> Schriftliche/Telefonische Bestellung (MOTO)	<input type="checkbox"/> Schriftliche/Telefonische Bestellung (MOTO)	
<input type="checkbox"/> E-Commerce	<input type="checkbox"/> E-Commerce	
<input type="checkbox"/> Vorlage der Karte (persönlich)	<input type="checkbox"/> 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 2b. Beschreibung des Zahlungskartengeschäfts

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

Teil 2c. Standorte

Listen Sie alle Einrichtungen und Standorte auf (beispielsweise Einzelhandelsgeschäfte, Büroräume, Rechenzentren, Callcenter), die in der PCI-DSS-Prüfung aufgelistet wurden.

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

Teil 2d. Zahlungsanwendung

Nutzt das Unternehmen eine oder mehrere Zahlungsanwendungen? Ja Nein

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

Name der Zahlungsanwendung	Versionsnummer	Anbieter der Anwendung	Steht die Anwendung auf der PA-DSS-Liste?	Ablaufdatum der PA-DSS-Liste (falls zutreffend)
			<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
			<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
			<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
			<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
			<input type="checkbox"/> Ja <input type="checkbox"/> 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?

Ja Nein

(Hinweise zur Netzwerksegmentierung finden Sie im PCI DSS im Abschnitt „Netzwerksegmentierung“.)

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:

Name des Dienstanbieters:	Beschreibung der erbrachten Dienstleistungen:

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

Teil 2g. Qualifikation zum Ausfüllen von SBF C

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

- Der Händler hat auf demselben Gerät und/oder demselben Local Area Network (LAN) ein Zahlungsanwendungssystem und eine Internetverbindung;
- das Gerät mit Zahlungsanwendungssystem/Internetverbindung ist nicht mit anderen Systemen in der Händlerumgebung verbunden;
- der physische Standort der POS-Umgebung ist nicht mit anderen Stellen oder Standorten verbunden, und jedes LAN ist nur für einen einzigen Standort eingerichtet;
- Der Händler speichert keine Karteninhaberdaten in elektronischem Format; **und**
- Wenn der Händler Karteninhaberdaten speichert, befinden sich diese nur in Berichten oder Kopien von Quittungen auf Papier und werden nicht elektronisch entgegengenommen.

2. Abschnitt: Selbstbeurteilungsfragebogen C

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

Selbstbeurteilung abgeschlossen am:

Erstellung und Wartung sicherer Netzwerke und Systeme

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

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
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 vertrauenswürdigen 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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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?	<ul style="list-style-type: none"> Standards für die Firewall- und Router-Konfiguration durchgehen Firewall- und Router-Konfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Verbietet die Firewall-Konfiguration wie folgt den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung?					
1.3.4	Ist die Weiterleitung ausgehenden Datenverkehrs von der Karteninhaberdaten-Umgebung an das Internet ausdrücklich erlaubt?	<ul style="list-style-type: none"> Firewall- und Router-Konfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Sind nur etablierte Verbindungen in das Netzwerk zulässig?	<ul style="list-style-type: none"> Firewall- und Router-Konfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation überprüfen ▪ Systemkonfigurationen und Kontoeinstellungen prüfen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(a) Werden vom Anbieter gelieferte Standardeinstellungen immer geändert, bevor ein System im Netzwerk installiert wird? <i>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.).</i>					
(b) Werden unnötige Standardkonten vor der Installation eines Systems im Netzwerk entfernt oder deaktiviert?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen und Kontoeinstellungen untersuchen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Für drahtlose Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder die Karteninhaberdaten übertragen, werden ALLE Standardeinstellungen des Wireless-Anbieters wie folgt geändert?				
(a) Werden Standardwerte der Verschlüsselungsschlüssel zum Zeitpunkt der Installation geändert und werden sie jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Werden Standard-SNMP-Community-Zeichenfolgen auf drahtlosen Geräten bei der Installation geändert?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Mitarbeiter befragen ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
(c) Werden Standardkennwörter/-sätze auf Zugriffspunkten bei der Installation geändert?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Wird die Firmware auf drahtlosen Geräten aktualisiert, um eine starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) Werden gegebenenfalls auch andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen geändert?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2 (a) Werden für alle Systemkomponenten Konfigurationsstandards entwickelt und sind diese mit den branchenüblichen Systemhärtungsstandards vereinbar? <i>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).</i>	<ul style="list-style-type: none"> ▪ Standards für die Systemkonfiguration durchgehen ▪ Branchenübliche Härtungsstandards durchgehen ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Werden die Systemkonfigurationsstandards gemäß Anforderung 6.1 aktualisiert, sobald neue Schwachstellen identifiziert werden?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Werden neue Systemkonfigurationsstandards angewendet, sobald neue Systeme konfiguriert werden?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
(d) Umfassen die festgelegten Konfigurationsstandards alle nachfolgenden Punkte? <ul style="list-style-type: none"> • 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 Sicherheitsniveaunanforderungen 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 	<ul style="list-style-type: none"> ▪ Standards für die Systemkonfiguration durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1 (a) Ist nur eine primäre Funktion pro Server implementiert, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveaunanforderungen existieren? <i>Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.</i>	<ul style="list-style-type: none"> ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(b) Wenn Virtualisierungstechnologien eingesetzt werden, ist pro virtuelle Systemkomponente oder Gerät nur eine primäre Funktion implementiert?	<ul style="list-style-type: none"> Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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)?	<ul style="list-style-type: none"> Konfigurationsstandards durchgehen Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sind alle aktivierten unsicheren Dienste, Daemons oder Protokolle durch die dokumentierten Konfigurationsstandards legitimiert?	<ul style="list-style-type: none"> Konfigurationsstandards durchgehen Mitarbeiter befragen Konfigurationseinstellungen untersuchen Aktivierte Dienste usw. mit den dokumentierten Rechtfertigungen vergleichen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Sind zusätzliche Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden, dokumentiert und implementiert? <i>Hinweis: Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.</i>	<ul style="list-style-type: none"> Konfigurationsstandards durchgehen Konfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(a) Verstehen sich Systemadministratoren und/oder Mitarbeiter, die Systemkomponenten konfigurieren, auf allgemeine Sicherheitsparametereinstellungen für diese Systemkomponenten?	<ul style="list-style-type: none"> Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sind in den Systemkonfigurationsstandards gängige Sicherheitsparametereinstellungen enthalten?	<ul style="list-style-type: none"> Standards für die Systemkonfiguration durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
(c) Sind die Sicherheitsparametereinstellungen auf den Systemkomponenten sachgemäß eingestellt?	<ul style="list-style-type: none"> ▪ Systemkomponenten untersuchen ▪ Sicherheitsparametereinstellungen untersuchen ▪ Einstellungen mit Systemkonfigurationsstandards vergleichen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5 (a) Wurden alle unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver entfernt?	<ul style="list-style-type: none"> ▪ Sicherheitsparameter auf Systemkomponenten untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Werden aktivierte Funktionen dokumentiert und sind sie sicher konfiguriert?	<ul style="list-style-type: none"> ▪ Dokumentation durchgehen ▪ Sicherheitsparameter auf Systemkomponenten untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Sind auf den Systemkomponenten ausschließlich dokumentierte Funktionen vorhanden?	<ul style="list-style-type: none"> ▪ Dokumentation durchgehen ▪ Sicherheitsparameter auf Systemkomponenten untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3 Ist der Nichtkonsolen-Verwaltungszugriff wie folgt verschlüsselt? <i>Hinweis: Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.</i>					
(a) Werden alle Nichtkonsolen-Verwaltungszugriffe mit einer starken Kryptographie verschlüsselt und wird eine starke Verschlüsselungsmethode aufgerufen, bevor das Administratorkennwort angefordert wird?	<ul style="list-style-type: none"> ▪ Systemkomponenten untersuchen ▪ Systemkonfigurationen untersuchen ▪ Administratoranmeldung überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Sind die Systemdienste und -parameterdateien so konfiguriert, dass die Nutzung von Telnet und anderen unsicheren Remote-Anmeldebefehlen verhindert wird?	<ul style="list-style-type: none"> ▪ Systemkomponenten untersuchen ▪ Dienste und Dateien untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
(c) Ist der Administratorzugriff auf die webbasierten Managementschnittstellen mit einer starken Kryptographie verschlüsselt?	<ul style="list-style-type: none"> ▪ Systemkomponenten untersuchen ▪ Administratoranmeldung überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Wird für die eingesetzte Technologie eine starke Kryptographie gemäß den bewährten Branchenverfahren und/oder Anbieterempfehlungen implementiert?	<ul style="list-style-type: none"> ▪ Systemkomponenten untersuchen ▪ Anbieterdokumentation durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.5 Sind Sicherheitsrichtlinien und betriebliche Verfahren zum Management der Anbieterstandardeinstellungen oder anderer Sicherheitsparameter ...? <ul style="list-style-type: none"> ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt 	<ul style="list-style-type: none"> ▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Systemkonfigurationen untersuchen ▪ Löschprozesse untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Halten alle Systeme die folgenden Anforderungen hinsichtlich des Verbots ein, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern (auch wenn diese verschlüsselt sind)?					
3.2.1	<p>Wird der gesamte Inhalt einer Spur auf dem Magnetstreifen (auf der Rückseite einer Karte, gleichwertige Daten auf einem Chip oder an einer anderen Stelle) nach der Autorisierung nicht gespeichert?</p> <p><i>Diese Daten werden auch als Spurdaten, Full-Track-Daten, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet.</i></p> <p>Hinweis: Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:</p> <ul style="list-style-type: none"> • Der Name des Karteninhabers, • Primäre Kontonummer (PAN), • Ablaufdatum und • Servicecode <p><i>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.</i></p>	<ul style="list-style-type: none"> ▪ Datenquellen untersuchen, insbesondere: <ul style="list-style-type: none"> • Eingehende Transaktionsdaten • Sämtliche Protokolle • Verlaufsdateien • Trace-Dateien • Datenbankschema • Datenbankinhalte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
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?	<ul style="list-style-type: none"> ▪ Datenquellen untersuchen, insbesondere: <ul style="list-style-type: none"> • Eingehende Transaktionsdaten • Sämtliche Protokolle • Verlaufsdateien • Trace-Dateien • Datenbankschema • Datenbankinhalte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Wird die persönliche Identifizierungsnummer (PIN) oder der verschlüsselte PIN-Block nach der Autorisierung nicht gespeichert?	<ul style="list-style-type: none"> ▪ Datenquellen untersuchen, insbesondere: <ul style="list-style-type: none"> • Eingehende Transaktionsdaten • Sämtliche Protokolle • Verlaufsdateien • Trace-Dateien • Datenbankschema • Datenbankinhalte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3	<p>Wird die PAN zum Teil verborgen (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), sodass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können?</p> <p>Hinweis: Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. bei juristischen Anforderungen und Anforderungen der Kreditkartenunternehmen an POS-Belege.</p>	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Die Rollen überprüfen, welche die vollständige PAN einsehen müssen. ▪ Systemkonfigurationen untersuchen ▪ PAN-Anzeigen beobachten 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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? <i>Hinweis: Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.</i> <i>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).</i>	<ul style="list-style-type: none"> ▪ Dokumentierte Standards durchgehen ▪ Richtlinien und Verfahren durchgehen ▪ Alle Standorte, an denen CHD übertragen oder empfangen wird, überprüfen ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Werden ausschließlich vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert?	<ul style="list-style-type: none"> ▪ Eingehende und ausgehende Übertragungen überprüfen ▪ Schlüssel und Zertifikate untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Sind Sicherheitsprotokolle implementiert, um ausschließlich sichere Konfigurationen zu verwenden und keine unsicheren Versionen oder Konfigurationen zu unterstützen?	<ul style="list-style-type: none"> ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Wird für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet (siehe Anbieterempfehlungen/bewährte Verfahren)?	<ul style="list-style-type: none"> ▪ Anbieterdokumentation durchgehen ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(e) Wird bei TLS-Implementierungen bei jeder Übertragung bzw. bei jedem Empfang von Karteninhaberdaten TLS aktiviert? <i>Bei browserbasierten Implementierungen ist beispielsweise Folgendes zu prüfen:</i> <ul style="list-style-type: none"> • Wird „HTTPS“ als Bestandteil des Browser-URL-Protokolls angezeigt? • Werden Karteninhaberdaten nur angefordert, wenn die URL die Komponente „HTTPS“ enthält? 	<ul style="list-style-type: none"> ▪ Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Werden bewährte Branchenverfahren eingesetzt, um eine starke Verschlüsselung in der Authentifizierung und Übertragung für drahtlose Netzwerke zu implementieren, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind?	<ul style="list-style-type: none"> ▪ Dokumentierte Standards durchgehen ▪ Drahtlose Netzwerke überprüfen ▪ Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(b) Sind Richtlinien vorhanden, die festlegen, dass ungeschützte PANs nicht über Messaging-Technologien für Endanwender gesendet werden dürfen?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Unterhaltung eines Anfälligkeits-Managementprogramms

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

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
5.1	Ist eine Antivirensoftware auf allen Systemen, die üblicherweise das Ziel böswilliger Software sind, implementiert?	<ul style="list-style-type: none"> Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Anbieterdokumentation durchgehen Systemkonfigurationen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Richtlinien und Verfahren untersuchen Antiviren-Konfigurationen einschließlich der Master-Installation untersuchen Systemkomponenten untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sind automatische Updates und regelmäßige Scans aktiviert und werden sie regelmäßig durchgeführt?	<ul style="list-style-type: none"> Antiviren-Konfigurationen einschließlich der Master-Installation untersuchen Systemkomponenten untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Generieren alle Virenschutzmechanismen Prüfprotokolle und werden die Protokolle gemäß PCI-DSS-Anforderung 10.7 aufbewahrt?	<ul style="list-style-type: none"> Antiviren-Konfigurationen untersuchen Prozesse zur Aufbewahrung von Protokollen durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
5.3 Aspekte bei Antivirenmechanismen: <ul style="list-style-type: none"> ▪ Werden alle Antivirenmechanismen aktiv ausgeführt? ▪ Sind sie gegen benutzerseitige Deaktivierungen oder Veränderungen gesichert? <p><i>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.</i></p>	<ul style="list-style-type: none"> ▪ Antiviren-Konfigurationen untersuchen ▪ Systemkomponenten untersuchen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.
<p>6.1 Gibt es einen Prozess zur Erkennung folgender und anderer Sicherheitsrisiken?</p> <ul style="list-style-type: none"> ▪ Nutzung verlässlicher externer Informationsquellen ▪ Zuweisung von Risikostufen für Sicherheitsrisiken mit der Ermittlung sämtlicher „hohen“ und „kritischen“ Risiken <p><i>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.</i></p> <p><i>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.</i></p>	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Prozesse überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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.	<ul style="list-style-type: none"> Richtlinien und Verfahren durchgehen Systemkomponenten untersuchen Liste der installierten Sicherheitspatches mit der Liste der neuesten Anbieterpatches vergleichen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.6	Werden alle relevanten PCI-DSS-Anforderungen nach Abschluss einer signifikanten Änderung auf allen neuen oder veränderten Systemen und Netzwerken implementiert und die Dokumentation entsprechend aktualisiert? Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.	<ul style="list-style-type: none"> Zurückverfolgen der Änderungen zur Dokumentation der Änderungskontrolle Durchsicht der Dokumentation zur Änderungskontrolle Mitarbeiter befragen Beobachten betroffener Systeme oder Netzwerke 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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? <ul style="list-style-type: none"> ▪ Auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind ▪ Exklusive Zuweisung zu Rollen, die diesen privilegierten Zugriff konkret benötigen 	<ul style="list-style-type: none"> ▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen ▪ Mitarbeiter befragen ▪ Management befragen ▪ Privilegierte Benutzer-IDs überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Werden Zugriffsberechtigungen anhand der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter zugewiesen?	<ul style="list-style-type: none"> ▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen ▪ Management befragen ▪ Benutzer-IDs überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> ▪ Kennwortverfahren überprüfen ▪ Mitarbeiterbefragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> ▪ Kennwortverfahren überprüfen ▪ Mitarbeiterbefragen ▪ Prozesse überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Werden die Fernzugriffskonten von Dritten während der Nutzung überwacht?	<ul style="list-style-type: none"> ▪ Mitarbeiterbefragen ▪ Prozesse überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.6	(a) Werden wiederholte Zugriffsversuche begrenzt, indem die Benutzer-ID nach mehr als sechs Versuchen gesperrt wird?	<ul style="list-style-type: none"> ▪ Kennwortverfahrenüberprüfen ▪ Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> ▪ Kennwortverfahrenüberprüfen ▪ Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> ▪ Kennwortverfahrenüberprüfen ▪ Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
8.2	<p>Werden neben der Zuweisung einer eindeutigen ID eine oder mehrere der folgenden Methoden eingesetzt, um alle Benutzer zu authentifizieren?</p> <ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Kennwortverfahren überprüfen ▪ Authentifizierungsprozesse überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.3	<p>(a) Sind Parameter für Benutzerkennwörter so konfiguriert, dass die Kennwörter/-sätze folgende Voraussetzungen erfüllen müssen?</p> <ul style="list-style-type: none"> • Kennwörter müssen mindestens sieben Zeichen umfassen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden. <p>Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.</p>	<ul style="list-style-type: none"> ▪ Systemkonfigurationseinstellungen zur Überprüfung der Kennwortparameter untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.4	<p>Werden Benutzerkennwörter/-sätze mindestens alle 90 Tage geändert?</p>	<ul style="list-style-type: none"> ▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.5	<p>Muss eine Person ein neues Kennwort/einen neuen Kennsatz einreichen, das/der sich von ihren letzten vier Kennwörtern/-sätzen unterscheidet?</p>	<ul style="list-style-type: none"> ▪ Kennwortverfahren überprüfen ▪ Systemkomponenten anhand von Stichproben überprüfen ▪ Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.6	<p>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?</p>	<ul style="list-style-type: none"> ▪ Kennwortverfahren überprüfen ▪ Systemkonfigurationseinstellungen untersuchen ▪ Sicherheitspersonal beobachten 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
8.3	<p>Sind alle Nichtkonsolen-Verwaltungszugriffe und alle Fernzugriffe auf das CDE wie folgt durch Multi-Faktor-Authentifizierung geschützt:</p> <p>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.</p>					
8.3.1	<p>Ist die Multi-Faktor-Authentifizierung fester Bestandteil für alle Nichtkonsolen-Zugriffe auf das CDE durch Mitarbeiter mit Verwaltungszugriff?</p> <p>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</p>	<ul style="list-style-type: none"> ▪ Systemkonfigurationen untersuchen ▪ Beobachten von Mitarbeitern bei der Anmeldung in die CDE 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3.2	<p>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)?</p>	<ul style="list-style-type: none"> ▪ Systemkonfigurationen untersuchen ▪ Beobachten von Mitarbeitern mit Fernzugriff 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4	<p>(a) Werden Authentifizierungsverfahren und -richtlinien dokumentiert und an alle Benutzer weitergegeben?</p>	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Verteilungsmethode überprüfen ▪ Mitarbeiter befragen ▪ Benutzer befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
(b) Sind folgende Punkte in den Authentifizierungsverfahren und -richtlinien enthalten? <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Dokumentation für Benutzer überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.5 Sind Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden wie folgt untersagt? <ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Benutzer-ID-Listen überprüfen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.8 Sind die Sicherheitsrichtlinien und betrieblichen Verfahren zur Identifizierung und Authentifizierung ...? <ul style="list-style-type: none"> ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt 	<ul style="list-style-type: none"> ▪ Sicherheitsrichtlinien und betriebliche Verfahren überprüfen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> ▪ Physische Zugangskontrollen überprüfen ▪ Mitarbeiter beobachten 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.1	(a) Wird der Zugang zu sensiblen Bereichen entweder mithilfe von Videokameras oder Kontrollsystemen (oder beidem) überwacht? <i>Hinweis: „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die öffentlichen Bereiche, in denen lediglich POS-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).</i>	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Physische Kontrollsysteme überprüfen ▪ Sicherheitsfunktionen überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sind entweder die Videokameras und/oder Zugangskontrollsysteme (oder beides) vor Manipulation oder Deaktivierung geschützt?	<ul style="list-style-type: none"> ▪ Prozesse überprüfen ▪ Mitarbeiterbefragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Werden die anhand von Videokameras und/oder Zugangskontrollmechanismen erfassten Daten überprüft und mit anderen Eingaben verglichen?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Sicherheitspersonalbefragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Werden die anhand von Videokameras und/oder Zugangskontrollmechanismen erfassten Daten mindestens für einen Zeitraum von drei Monaten gespeichert, sofern keine anderweitige gesetzliche Regelung zutrifft?	<ul style="list-style-type: none"> ▪ Prozesse zur Aufbewahrung von Daten überprüfen ▪ Datenspeicherungüberprüfen ▪ Sicherheitspersonalbefragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
9.1.2	<p>Sind physische und/oder logische Kontrollen zur Beschränkung des Zugriffs auf öffentlich zugängliche Netzwerkbuchsen implementiert?</p> <p><i>Beispielsweise sollte die Möglichkeit bestehen, Netzwerkbuchsen in für Besucher zugänglichen Bereichen zu deaktivieren und nur dann zu aktivieren, wenn der Netzwerkzugriff ausdrücklich zugelassen ist. Alternativ können auch Prozesse implementiert werden, mit denen Besucher jederzeit in Bereiche mit aktiven Netzwerkbuchsen geleitet werden.</i></p>	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Mitarbeiter befragen ▪ Orte beobachten 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	<p>Wird die physische Sicherheit aller Medien gewährleistet (insbesondere Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)?</p> <p><i>Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Medien“ auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.</i></p>	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren zur physischen Sicherung von Medien durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6	(a) Wird die interne oder externe Verteilung jeglicher Art von Medien stets strikt kontrolliert?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren zur Verteilung von Medien durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Umfassen die Kontrollen folgende Punkte?					
9.6.1	Werden Medien klassifiziert, sodass die Sensibilität der Daten bestimmt werden kann?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren zur Klassifizierung von Medien durchgehen ▪ Sicherheitspersonal befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Protokolle und Dokumentation zur Verteilung von Medien untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	Wird vor dem Verlagern von Medien die Genehmigung des Managements eingeholt (insbesondere wenn Medien an Einzelpersonen verteilt werden)?	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Protokolle und Dokumentation zur Verteilung von Medien untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	Werden strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durchgeführt?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
9.8	(a) Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Erfolgt die Vernichtung von Medien wie nachstehend beschrieben?					
9.8.1	(a) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?	<ul style="list-style-type: none"> • Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen • Mitarbeiter befragen • Prozesse überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Werden Container zur Aufbewahrung von zu vernichtenden Informationen so geschützt, dass Zugriffe auf diese Inhalte vermieden werden?	<ul style="list-style-type: none"> • Sicherheit von Containern überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	Sind die Geräte, die Zahlungskartendaten über eine direkte physische Interaktion mit der Karte erfassen, vor Manipulation und Austausch geschützt? <i>Hinweis: Diese Anforderung gilt für Kartenlesegeräte, die bei Transaktionen eingesetzt werden, bei denen die Karte am Point-of-Sale vorliegt und durch das Gerät gezogen oder in das Gerät eingesteckt werden muss. Diese Anforderung gilt nicht für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke.</i>					
	(a) Sehen Richtlinien und Verfahren das Führen einer Liste solcher Geräte vor?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sehen Richtlinien und Verfahren vor, dass Geräte regelmäßig auf Manipulations- oder Austauschversuche untersucht werden?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Sehen Richtlinien und Verfahren vor, dass das Bewusstsein der Mitarbeiter für verdächtiges Verhalten und das Melden der Manipulation bzw. des Austauschs von Geräten gefördert werden?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
9.9.1 (a) Enthält die Geräteliste folgende Angaben? <ul style="list-style-type: none"> Fabrikat und Modell des Geräts Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet) Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung 	<ul style="list-style-type: none"> Geräteliste überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Ist die Liste korrekt, vollständig und aktuell?	<ul style="list-style-type: none"> Geräte und Gerätestandorte prüfen und mit der Liste vergleichen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Wird die Geräteliste aktualisiert, sobald Geräte hinzugefügt, an einen anderen Standort gebracht, außer Betrieb genommen werden usw.?	<ul style="list-style-type: none"> Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.2 (a) Werden Geräteoberflächen regelmäßig auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch untersucht (stimmen beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht)? <i>Hinweis: Anzeichen für eine Manipulation oder den Austausch von Geräten sind zum Beispiel unerwartete Anbauten oder Kabel, fehlende oder geänderte Sicherheitssiegel, beschädigte oder andersfarbige Gehäuse bzw. Änderungen bei der Seriennummer oder anderen externen Kennzeichen.</i>	<ul style="list-style-type: none"> Mitarbeiter befragen Untersuchungsprozesse beobachten und mit festgelegten Prozessen vergleichen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Kennen die Mitarbeiter die Verfahren zur Untersuchung von Geräten?	<ul style="list-style-type: none"> Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
		Ja	Ja, mit CCW	Nein	Nicht zutr.	
9.9.3	Wurde das Bewusstsein der Mitarbeiter für Manipulations- oder Austauschversuche insbesondere durch die nachfolgenden Punkte gefördert?					
(a)	<p>Umfasst das Schulungsmaterial für die Mitarbeiter an POS-Standorten die folgenden Punkte?</p> <ul style="list-style-type: none"> • Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten). • Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe. • Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen). • Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter). 	<ul style="list-style-type: none"> ▪ Schulungsmaterialien überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b)	Wurden die Mitarbeiter an POS-Standorten geschult und haben sie die Verfahren zur Erkennung und Meldung von Versuchen der Manipulation oder des Austauschs von Geräten verinnerlicht?	<ul style="list-style-type: none"> ▪ Mitarbeiter an POS-Standorten befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.
10.2	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	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	Ungültige logische Zugriffsversuche	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Werden die folgenden Audit-Trail-Einträge für alle Systemkomponenten für jedes Ereignis aufgezeichnet?					
10.3.1	Benutzeridentifizierung	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	Ereignistyp	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
10.3.3	Datum und Uhrzeit	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.4	Erfolgs- oder Fehleranzeige	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.5	Ereignisursprung	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen ▪ Einstellungen für Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Werden Protokolle und Sicherheitsereignisse für alle Systemkomponenten auf Unregelmäßigkeiten oder verdächtige Aktivitäten überprüft? Hinweis: Um die Konformität mit Anforderung 10.6 zu erzielen, können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.					

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
10.6.1	(b) Werden die folgenden Protokolle und Sicherheitsereignisse mindestens täglich manuell oder mittels Protokolltools überprüft? <ul style="list-style-type: none"> • 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.) 	<ul style="list-style-type: none"> ▪ Sicherheitsrichtlinien und -verfahren durchgehen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.2	(b) Werden Protokolle aller weiteren Systemkomponenten regelmäßig – manuell oder mittels Protokolltools – anhand der Richtlinien und Risikomanagementstrategie des Unternehmens überprüft?	<ul style="list-style-type: none"> ▪ Sicherheitsrichtlinien und -verfahren durchgehen ▪ Dokumentation zur Risikobeurteilung durchgehen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.3	(b) Werden die bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten nachverfolgt?	<ul style="list-style-type: none"> ▪ Sicherheitsrichtlinien und -verfahren durchgehen ▪ Prozesse überprüfen ▪ Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7	(b) Werden Prüfprotokolle mindestens ein Jahr aufbewahrt?	<ul style="list-style-type: none"> ▪ Sicherheitsrichtlinien und -verfahren durchgehen ▪ Mitarbeiter befragen ▪ Prüfprotokolle überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Sind die Protokolle zu Analysezwecken mindestens drei Monate lang unmittelbar verfügbar?	<ul style="list-style-type: none"> ▪ Mitarbeiter befragen ▪ Prozesse überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.
11.1	(a) Werden Prozesse zur Erkennung und Identifizierung von autorisierten und nicht autorisierten WLAN-Zugriffspunkten vierteljährlich implementiert? <i>Hinweis: Methoden, die sich hierfür anbieten, sind unter anderen Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme. Welche Methode auch immer verwendet wird, sie muss ausreichend sein, um jegliche nicht autorisierten Geräte zu erkennen und zu identifizieren.</i>	<ul style="list-style-type: none"> Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Ist die angewandte Methodik ausreichend, um jegliche nicht autorisierte Zugriffspunkte für drahtlose Netzwerke, einschließlich mindestens folgender Elemente, zu erkennen und zu identifizieren? <ul style="list-style-type: none"> In Systemkomponenten eingefügte WLAN-Karten; an Systemkomponenten angeschlossene tragbare Geräte (z. B. durch USB), mit denen ein WLAN-Zugriffspunkt eingerichtet wird; und an einen Netzwerkport oder ein Netzwerkgerät angeschlossene Drahtlosgeräte. 	<ul style="list-style-type: none"> Methodik evaluieren 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Werden Wireless-Scans zur Identifizierung nicht autorisierter WLAN-Zugriffspunkte mindestens vierteljährlich auf allen Systemkomponenten und an allen Stellen durchgeführt?	<ul style="list-style-type: none"> Ergebnisse der letzten WLAN-Untersuchungen überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Falls eine automatische Überwachung eingesetzt wird (z. B. ein Wireless IDS/IPS-System, NAC usw.), sind in der Konfiguration Alarmmeldungen für das Personal vorgesehen?	<ul style="list-style-type: none"> Konfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
11.1.1	Werden die autorisierten WLAN-Zugriffspunkte inventarisiert und ist zu jedem Zugriffspunkt eine geschäftliche Begründung dokumentiert?	<ul style="list-style-type: none"> ▪ Inventar und Unterlagen überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.2	(a) Ist im Vorfalleaktionsplan eine Reaktion für den Fall definiert und vorgesehen, dass ein nicht autorisierter WLAN-Zugriffspunkt entdeckt wird?	<ul style="list-style-type: none"> ▪ Vorfalleaktionsplan untersuchen (siehe Anforderung 12.10) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Werden Maßnahmen getroffen, wenn nicht autorisierte WLAN-Zugriffspunkte gefunden werden?	<ul style="list-style-type: none"> ▪ Verantwortliche Mitarbeiter befragen ▪ Letzte WLAN-Untersuchungen (Scans) und daraufhin erfolgte Reaktionen überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2	<p>Werden wie folgt interne und externe Netzwerkanfälligkeitsscans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Modifizierungen von Firewall-Regeln, Produktupgrades) ausgeführt?</p> <p>Hinweis: Um beim vierteljährlichen Scan sämtliche Systeme und alle möglichen Sicherheitsrisiken zu berücksichtigen, können mehrere Scan-Berichte miteinander kombiniert werden. Es ist unter Umständen zusätzliche Dokumentation erforderlich, um zu belegen, dass bei noch nicht behobenen Sicherheitsrisiken erste Schritte unternommen wurden.</p> <p>Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier vierteljährliche Scans bestanden sein müssen, wenn der Prüfer feststellt, dass 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Einheit über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle in den Scan-Ergebnissen festgestellten Sicherheitsrisiken nachweislich korrigiert wurden. Für die Folgejahre nach der ersten PCI-DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.</p>					

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
11.2.1	(a) Werden vierteljährlich interne Schwachstellenprüfungen durchgeführt?	▪ Scan-Berichte durchgehen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Behandelt der vierteljährliche interne Scanprozess alle „schwerwiegenden“ Sicherheitslücken und sieht erneute Scans vor, bis diese (gemäß PCI-DSS-Anforderung 6.1) gelöst wurden?	▪ Scan-Berichte durchgehen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Werden die internen vierteljährlichen Scans von (einem) dafür qualifizierten internen Mitarbeiter(n) oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	▪ Mitarbeiter befragen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2	(a) Werden vierteljährlich externe Schwachstellenprüfungen (Scans) durchgeführt? <i>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.</i>	▪ Ergebnisse der externen Schwachstellenprüfungen aus den vorangegangenen vier Quartalen durchgehen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Erfüllen die Ergebnisse der vierteljährlichen externen Prüfungen und erneuten Prüfungen die Anforderungen des ASV-Programtleitfadens (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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
11.2.3 (a) Werden nach jeder wesentlichen Änderung interne und externe Prüfungen und nach Bedarf erneute Prüfungen durchgeführt? <i>Hinweis: Scans müssen von qualifizierten Mitarbeitern durchgeführt werden.</i>	<ul style="list-style-type: none"> Änderungskontrolldokumentation und Scan-Berichte überprüfen und zuordnen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.3 (b) Sieht der Scanprozess erneute Scans vor, bis ... <ul style="list-style-type: none"> ... bei externen Scans keine Sicherheitsrisiken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung höher als 4.0 bewertet wurden, ... bei internen Scans der Fehler behoben wurde oder alle „schwerwiegenden“ Sicherheitslücken, wie in der PCI-DSS-Anforderung 6.1 dargelegt, gelöst wurden? 	<ul style="list-style-type: none"> Scan-Berichte durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.3 (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)?	<ul style="list-style-type: none"> Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.4 Falls die CDE durch Segmentierung von anderen Netzwerken isoliert wird:					
11.3.4 (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?	<ul style="list-style-type: none"> Segmentierungskontrollen überprüfen Methodik für Penetrationstests überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	<p>(b) Erfüllen die Penetrationstests zur Überprüfung der Segmentierungskontrollen die folgenden Voraussetzungen?</p> <ul style="list-style-type: none"> Die Tests werden mindestens einmal jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt. Bei den Tests werden alle angewendeten Segmentierungskontrollen/-methoden geprüft. Es wird geprüft, ob die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden. 	<ul style="list-style-type: none"> Ergebnisse des letzten Penetrationstests untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<p>(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)?</p>	<ul style="list-style-type: none"> Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5	<p>(a) Wird ein System zur Erkennung von Änderungen (z. B. Tools zur Überwachung der Dateintegrität) bereitgestellt, um nicht autorisierte Änderungen (einschließlich Änderungen, Ergänzungen und Löschungen) an wichtigen System-, Konfigurations- oder Inhaltsdateien zu erkennen?</p> <p><i>Dateien, die überwacht werden sollten, sind u. a.:</i></p> <ul style="list-style-type: none"> 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.) 	<ul style="list-style-type: none"> Systemeinstellungen und überwachte Dateien beobachten Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	<p>(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?</p> <p>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 Dienstleister) beurteilt und definiert werden.</p>	<ul style="list-style-type: none"> Systemeinstellungen und überwachte Dateien beobachten Ergebnisse der Überwachung durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5.1	Wurde ein Prozess implementiert, um auf Alarme der Änderungserkennungslösung reagieren zu können?	<ul style="list-style-type: none"> Systemkonfigurationseinstellungen untersuchen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> Informationssicherheitsrichtlinie überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.1	Wird die Sicherheitsrichtlinie mindestens einmal pro Jahr überarbeitet und bei Umgebungsänderungen aktualisiert?	<ul style="list-style-type: none"> Informationssicherheitsrichtlinie überprüfen Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	<p>Wurden Nutzungsrichtlinien für wichtige Technologien entwickelt, um die ordnungsgemäße Nutzung dieser Technologien zu regeln – unter Berücksichtigung der nachfolgenden Punkte?</p> <p>Hinweis: Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.</p>					
12.3.1	Ausdrückliche Genehmigung durch autorisierte Parteien, diese Technologien zu nutzen	<ul style="list-style-type: none"> Nutzungsrichtlinien überprüfen Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	Authentifizierung zur Verwendung der Technologien	<ul style="list-style-type: none"> Nutzungsrichtlinien überprüfen Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	Eine Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	<ul style="list-style-type: none"> Nutzungsrichtlinien überprüfen Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	Akzeptable Nutzung dieser Technologien	<ul style="list-style-type: none"> Nutzungsrichtlinien überprüfen Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	Akzeptable Netzwerkorte für die Technologien	<ul style="list-style-type: none"> Nutzungsrichtlinien überprüfen Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
12.3.8	Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität	<ul style="list-style-type: none"> ▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.9	Aktivierung von Remotezugriff-Technologien für Anbieter und Geschäftspartner nur, wenn bei Anbietern und Geschäftspartnern ein dringender Bedarf besteht und die Technologie nach der Nutzung gleich wieder deaktiviert wird.	<ul style="list-style-type: none"> ▪ Nutzungsrichtlinien überprüfen ▪ Verantwortliche Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	<ul style="list-style-type: none"> ▪ Informationssicherheitsrichtlinie und -verfahren überprüfen ▪ Per Stichprobe ausgewählte Mitarbeiter befragen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> ▪ Informationssicherheitsrichtlinie und -verfahren überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6	(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheitsrichtlinien und Verfahren der Karteninhaberdaten zu vermitteln?	<ul style="list-style-type: none"> ▪ Sicherheitsbewusstseinsprogramm durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstleistern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert und gepflegt?					
12.8.1	Wird eine Liste von Dienstleistern mit Angabe einer Beschreibung der geleisteten Dienstleistung(en) gepflegt?	<ul style="list-style-type: none"> ▪ Richtlinien und Verfahren durchgehen ▪ Prozesse überprüfen ▪ Liste der Dienstleister überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
12.8.2	<p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> Schriftliche Vereinbarungen überprüfen Richtlinien und Verfahren durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Prozesse überprüfen Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	Gibt es ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard?	<ul style="list-style-type: none"> Prozesse überprüfen Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	Werden Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden, aufbewahrt?	<ul style="list-style-type: none"> Prozesse überprüfen Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> ▪ Vorfallreaktionsplan überprüfen ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Umfasst der Plan mindestens die folgenden Punkte?					
	<ul style="list-style-type: none"> • Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken; 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • konkrete Verfahren für die Reaktion auf Vorfälle; 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs; 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • Verfahren zur Datensicherung; 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen; 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • Abdeckung sämtlicher wichtigen Systemkomponenten; 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle. 	<ul style="list-style-type: none"> ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Anhang A: Zusätzliche PCI DSS Anforderungen

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

Dieser Anhang wird nicht für Händlerbeurteilungen verwendet.

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

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
A2.1 <i>Für POS POI -Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese Verbinden), die SSL und/oder eine frühe Version von TLS verwenden:</i> <ul style="list-style-type: none"> • Ist bestätigt, dass die Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind <li style="padding-left: 20px;"><i>Oder:</i> • Gibt es einen offiziellen Plan zur Risikoabschwächung und Migration gemäß Anforderung A2.2? 	<ul style="list-style-type: none"> ▪ Dokumentation dahingehend überprüfen (beispielsweise Anbieterdokumentation, Details der System-/Netzwerkconfiguration usw.), dass die POS POI-Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI-DSS-Frage	Erwartete Tests	Antwort (je Frage eine Antwort markieren)				
		Ja	Ja, mit CCW	Nein	Nicht zutr.	
A2.2	<p>Gibt es einen offiziellen Plan zur Risikoabschwächung und Migration für alle Implementierungen, die SSL und/oder eine frühe Version von TLS (anders als in A2.1 erlaubt) verwenden, der Folgendes umfasst:</p> <ul style="list-style-type: none"> ▪ Beschreibung der Verwendung, einschließlich; Art der verarbeiteten Daten, Arten und Anzahl der Systeme, die SSL/eine frühe Version von TLS verwenden/unterstützen, Art der Umgebung; ▪ Ergebnisse der Risikobewertung und vorhandene Kontrollen zur Risikominderung; ▪ Beschreibung der Prozesse zur Überwachung neuer Schwachstellen in Zusammenhang mit SSL/einer frühen Version von TLS; ▪ Beschreibung der Verfahren zur Änderungskontrolle, die implementiert wurden, um zu gewährleisten, dass SSL/eine frühe Version von TLS nicht in neuen Umgebungen implementiert wird; ▪ Einen Überblick über den Migrationsprojektplan, einschließlich einem Termin für den Abschluss der Migration, nicht später als der 30. Juni 2018? 	<ul style="list-style-type: none"> ▪ Überprüfen Sie den dokumentierten Plan zur Risikoabschwächung und Migration 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

3. Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

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

Auf der Grundlage der Ergebnisse des SBF C 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**):

<input type="checkbox"/>	<p>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.</p>						
<input type="checkbox"/>	<p>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.</p> <p>Zieldatum für Konformität:</p> <p>Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. <i>Sprechen Sie sich mit Ihrem Acquirer oder Ihrem/Ihren Kartenunternehmen ab, bevor Sie Teil 4 ausfüllen.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>Falls diese Option markiert ist, arbeiten Sie folgende Punkte ab:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 35%;">Betroffene Anforderung</th> <th>Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	Betroffene Anforderung	Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern				
Betroffene Anforderung	Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern						

Teil 3a. Feststellung des Status

Unterzeichner bestätigt:
(Zutreffendes ankreuzen)

<input type="checkbox"/>	Der PCI-DSS Selbstbeurteilungsfragebogen C, Version (Version des SBF), wurde den enthaltenen Anleitungen gemäß ausgefüllt.
<input type="checkbox"/>	Alle Informationen im oben genannten SBF und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung in allen materiellen Aspekten korrekt dar.
<input type="checkbox"/>	Mein Zahlungsanwendungsanbieter hat mir bestätigt, dass in meinem Zahlungssystem nach der Autorisierung keine empfindlichen Authentifizierungsdaten gespeichert werden.
<input type="checkbox"/>	Ich habe den PCI DSS gelesen und erkenne an, dass ich jederzeit die für meine Umgebung geltende PCI-DSS-Konformität aufrechterhalten muss.
<input type="checkbox"/>	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)

- | | |
|--------------------------|--|
| <input type="checkbox"/> | Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung vollständige Spurdaten („Full-Track-Daten“) ² , CAV2-, CVC2-, CID-, CVV2 ³ - oder PIN-Daten ⁴ gespeichert wurden. |
| <input type="checkbox"/> | ASV-Scans werden vom PCI SSC Approved Scanning Vendor (<i>Name des ASV</i>) durchgeführt. |

Teil 3b. Bescheinigung des Händlers

<i>Unterschrift des Beauftragten des Händlers</i> ↑	<i>Datum:</i>
<i>Name des Beauftragten des Händlers:</i>	<i>Titel:</i>

Teil 3c. Bestätigung durch den QSA (Qualified Security Assessor) (sofern zutreffend)

Falls ein QSA an dieser Beurteilung beteiligt war, beschreiben Sie bitte dessen Aufgabe:	
--	--

<i>Unterschrift des ordnungsgemäß ermächtigten Vertreters des QSA Unternehmens</i> ↑	<i>Datum:</i>
<i>Name des ordnungsgemäß ermächtigten Vertreters:</i>	<i>Unternehmen des QSA:</i>

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:	
---	--

² 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.

³ 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.

⁴ 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	<input type="checkbox"/>	<input type="checkbox"/>	
3	Schutz gespeicherter Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	<input type="checkbox"/>	<input type="checkbox"/>	
5	Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen	<input type="checkbox"/>	<input type="checkbox"/>	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	<input type="checkbox"/>	<input type="checkbox"/>	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten	<input type="checkbox"/>	<input type="checkbox"/>	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	<input type="checkbox"/>	<input type="checkbox"/>	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	<input type="checkbox"/>	<input type="checkbox"/>	
12	Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.	<input type="checkbox"/>	<input type="checkbox"/>	

Anhang A2	Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden	<input type="checkbox"/>	<input type="checkbox"/>	
-----------	--	--------------------------	--------------------------	--

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

