

**Payment Card Industry (PCI)  
Datensicherheitsstandard**

# **Selbstbeurteilungsfragebogen A und Konformitätsbescheinigung**

---

**Händler: Karte liegt nicht vor,  
alle Karteninhaber-Datenfunktionen extern  
vergeben**

**Zur Verwendung mit PCI DSS Version 3.2**

April 2016

## Dokumentänderungen

Datum	PCI DSS Version	SBF Revision	Beschreibung
Oktober 2008	1.2		Anpassung der Inhalte an den neuen PCI DSS v1.2 und Implementieren kleinerer Änderungen nach der Ursprungsversion v1.1.
Oktober 2010	2.0		Anpassung der Inhalte an die neuen Anforderungen und Testverfahren nach PCI DSS v2.0.
Februar 2014	3.0		Anpassung der Inhalte an die Anforderungen und Testverfahren nach PCI DSS v3.0 sowie Integration weiterer Reaktionsmöglichkeiten.
April 2015	3.1		Aktualisiert im Sinne des PCI-DSS v3.1. Ausführliche Informationen finden Sie unter <i>PA-DSS – Änderungsübersicht von PA-DSS Version 3.0 auf 3.1</i> .
Juli 2015	3.1	1.1	Aktualisierte Versionsnummerierung zur Abstimmung mit anderen SBF.
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> .

# Inhalt

---

<b>Document Changes .....</b>	<b>i</b>
<b>Before You Begin.....</b>	<b>iii</b>
<b>PCI DSS Self-Assessment Completion Steps .....</b>	<b>iii</b>
<b>Understanding the Self-Assessment Questionnaire .....</b>	<b>iv</b>
<i>Expected Testing .....</i>	<i>iv</i>
<b>Completing the Self-Assessment Questionnaire .....</b>	<b>v</b>
<b>Guidance for Non-Applicability of Certain, Specific Requirements.....</b>	<b>v</b>
<b>Legal Exception .....</b>	<b>v</b>
<b>Section 1: Assessment Information .....</b>	<b>1</b>
<b>Section 2: Self-Assessment Questionnaire A.....</b>	<b>5</b>
<b>Build and Maintain a Secure Network and Systems .....</b>	<b>5</b>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....</i>	<i>5</i>
<b>Implement Strong Access Control Measures.....</b>	<b>6</b>
<i>Requirement 8: Identify and authenticate access to system components .....</i>	<i>6</i>
<i>Requirement 9: Restrict physical access to cardholder data .....</i>	<i>7</i>
<b>Maintain an Information Security Policy .....</b>	<b>9</b>
<i>Requirement 12: Maintain a policy that addresses information security for all personnel .....</i>	<i>9</i>
<b>Appendix A: Additional PCI DSS Requirements .....</b>	<b>11</b>
<i>Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.....</i>	<i>11</i>
<i>Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS .....</i>	<i>11</i>
<i>Appendix A3: Designated Entities Supplemental Validation (DESV).....</i>	<i>11</i>
<b>Appendix B: Compensating Controls Worksheet.....</b>	<b>12</b>
<b>Appendix C: Explanation of Non-Applicability.....</b>	<b>13</b>
<b>Section 3: Validation and Attestation Details .....</b>	<b>14</b>

## Vorbereitung

---

SBF A zielt auf die Anforderungen von Händlern ab, deren Karteninhaber-Datenfunktionen vollständig an validierte Dritte vergeben werden und die lediglich Papierdokumente oder -quittungen mit Karteninhaberdaten aufbewahren.

SBF-A-Händler können E-Commerce- bzw. Versandhändler (Post-/Telefonbestellung, Karte liegt nicht vor) sein. Diese Händler speichern, verarbeiten oder übertragen keine Karteninhaberdaten in elektronischem Format auf ihren Systemen oder an ihrem Standort.

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

- Ihr Unternehmen akzeptiert nur Transaktionen, bei denen die Karte nicht physisch vorliegt (E-Commerce oder Versandhandel);
- Die Verarbeitung von Karteninhaberdaten wird vollständig an einen nach PCI DSS validierten externen Dienstleister vergeben;
- Ihr Unternehmen speichert, verarbeitet oder überträgt Karteninhaberdaten weder vor Ort noch auf Ihren Systemen in elektronischer Form, sondern verlässt sich voll und ganz auf einen oder mehrere Drittunternehmen, die diese Funktionen übernehmen;
- Ihr Unternehmen hat bestätigt, dass die Speicherung, Verarbeitung und/oder Übertragung der Karteninhaberdaten durch das oder die Drittunternehmen PCI-DSS-konform sind; **und**
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, sind in Papierform (zum Beispiel Papierdokumente und -quittungen), und diese Dokumente werden nicht elektronisch entgegengenommen.

*Für E-Commerce-Kanäle gilt zusätzlich:*

- Sämtliche Elemente der Zahlungsseiten, die an den Browser des Verbrauchers übermittelt werden, stammen ausschließlich und unmittelbar von einem nach PCI DSS validierten externen Dienstleister.

### ***Dieser SBF gilt nicht für den persönlichen Zahlungsverkehr.***

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. Abschnitt (Teil 1 und 2 der Konformitätsbescheinigung) – Informationen zur Beurteilung und Executive Summary.
  - 2. Abschnitt – PCI-DSS-Selbstbeurteilungsfragebogen (SBF A)

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

Diese und weitere Ressourcen sind auf der PCI-SSC-Website ([www.pcisecuritystandards.org](http://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?
<b>Ja</b>	Die erwarteten Tests wurden durchgeführt und alle Elemente der Anforderung wurden wie angegeben erfüllt.
<b>Ja, mit CCW</b> (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.
<b>Nein</b>	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.
<b>Nicht zutr.</b> (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

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 und Supermärkte	<input type="checkbox"/> Telekommunikation	<input type="checkbox"/> Lebensmitteleinzelhandel
<input type="checkbox"/> Erdöl/Erdgas (MOTO)	<input type="checkbox"/> E-Commerce	<input type="checkbox"/> Schriftliche/Telefonische Bestellung
<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"/> E-Commerce<br><input type="checkbox"/> Vorlage der Karte (persönlich) | <input type="checkbox"/> Schriftliche/Telefonische Bestellung (MOTO)<br><input type="checkbox"/> E-Commerce<br><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

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

Art der Einrichtung	Anzahl der Einrichtungen dieser Art	Standort(e) der Einrichtung (Ort, Land)
<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?  
(Hinweise zur Netzwerksegmentierung finden Sie im PCI DSS im Abschnitt „Netzwerksegmentierung“.)

Ja  Nein

**Teil 2f. Externe Dienstanbieter**

Verwendet Ihr Unternehmen einen Qualified Integrator & Reseller (QIR)?

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. Berechtigung zum Ausfüllen des SBF A**

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

- Der Händler akzeptiert nur Transaktionen, bei denen die Karte nicht physisch vorliegt (E-Commerce oder Versandhandel);
- die Verarbeitung von Karteninhaberdaten wird vollständig an einen nach PCI DSS validierten externen Dienstanbieter vergeben;
- der Händler speichert, verarbeitet oder überträgt keine Karteninhaberdaten in elektronischer Form, weder vor Ort noch auf seinen Systemen, sondern verlässt sich voll und ganz auf einen oder mehrere Dritte, der/die diese Funktionen übernimmt/übernehmen;

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | der Händler hat bestätigt, dass die Speicherung, Verarbeitung und/oder Übertragung der Karteninhaberdaten durch das oder die Drittunternehmen PCI-DSS-konform sind; <b>und</b>   |
| <input type="checkbox"/> | der Händler bewahrt ausschließlich Papierdokumente oder -quittungen mit Karteninhaberdaten auf und diese Dokumente werden nicht elektronisch empfangen.  |
| <input type="checkbox"/> | <i>Für E-Commerce-Kanäle gilt zusätzlich:</i><br>Sämtliche Elemente der Zahlungsseiten, die an den Browser des Verbrauchers übermittelt werden, stammen ausschließlich und unmittelbar von einem nach PCI DSS validierten externen Dienstanbieter. |

## 2. Abschnitt: Selbstbeurteilungsfragebogen A

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

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
2.1	(a) Werden vom Anbieter gelieferte Standardeinstellungen immer geändert, bevor ein System im Netzwerk installiert wird?  <i>Dies gilt für SÄMTLICHE Standardkennwörter, wie etwa die von Betriebssystemen, Sicherheitssoftware, Anwendungs- und Systemkonten, POS (Point of Sale, Verkaufsstelle)-Terminals, Zahlungsanwendungsb, SNMP (Simple Network Management Protocol)-Community-Zeichenfolgen usw.).</i>	<ul style="list-style-type: none"> <li>▪ Richtlinien und Verfahren durchgehen</li> <li>▪ Anbieterdokumentation überprüfen</li> <li>▪ Systemkonfigurationen und Kontoeinstellungen prüfen</li> <li>▪ Mitarbeiter befragen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Werden unnötige Standardkonten vor der Installation eines Systems im Netzwerk entfernt oder deaktiviert?	<ul style="list-style-type: none"> <li>▪ Richtlinien und Verfahren durchgehen</li> <li>▪ Anbieterdokumentation durchgehen</li> <li>▪ Systemkonfigurationen und Kontoeinstellungen untersuchen</li> <li>▪ Mitarbeiter befragen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Implementierung starker Zugriffskontrollmaßnahmen

### 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.
8.1.1	Wurde allen Benutzern eine eindeutige ID zugewiesen, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wurde?	<ul style="list-style-type: none"> <li>▪ Kennwortverfahren überprüfen</li> <li>▪ Mitarbeiter befragen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	Wird der Zugriff ehemaliger Benutzer sofort deaktiviert oder entfernt?	<ul style="list-style-type: none"> <li>▪ Kennwortverfahren überprüfen</li> <li>▪ Deaktivierte Benutzerkonten untersuchen</li> <li>▪ Aktuelle Zugriffslisten überprüfen</li> <li>▪ Zurückgegebene physische Authentifizierungsgeräte überprüfen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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"> <li>▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz;</li> <li>▪ etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard;</li> <li>▪ etwas, das Sie sind, wie zum Beispiel biometrische Daten.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Kennwortverfahren überprüfen</li> <li>▪ Authentifizierungsprozesse überprüfen</li> </ul>	<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"> <li>• Kennwörter müssen mindestens sieben Zeichen umfassen.</li> <li>• Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.</li> </ul> <p>Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.</p>	<ul style="list-style-type: none"> <li>▪ Systemkonfigurationseinstellungen zur Überprüfung der Kennwortparameter untersuchen</li> </ul>	<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.
8.5	<p>Sind Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden wie folgt untersagt?</p> <ul style="list-style-type: none"> <li>▪ Allgemeine Benutzer-IDs und -konten wurden deaktiviert oder entfernt;</li> <li>▪ es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen; und</li> <li>▪ es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Richtlinien und Verfahren durchgehen</li> <li>▪ Benutzer-ID-Listen überprüfen</li> <li>▪ Mitarbeiter befragen</li> </ul>	<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.
9.5	<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"> <li>▪ Richtlinien und Verfahren zur physischen Sicherung von Medien durchgehen</li> <li>▪ Mitarbeiter befragen</li> </ul>	<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"> <li>▪ Richtlinien und Verfahren zur Verteilung von Medien durchgehen</li> </ul>	<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"> <li>▪ Richtlinien und Verfahren zur Klassifizierung von Medien durchgehen</li> <li>▪ Sicherheitspersonal befragen</li> </ul>	<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.
9.6.2	Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?	<ul style="list-style-type: none"> <li>Mitarbeiter befragen</li> <li>Protokolle und Dokumentation zur Verteilung von Medien untersuchen</li> </ul>	<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"> <li>Mitarbeiter befragen</li> <li>Protokolle und Dokumentation zur Verteilung von Medien untersuchen</li> </ul>	<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"> <li>Richtlinien und Verfahren durchgehen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?	<ul style="list-style-type: none"> <li>Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen</li> </ul>	<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"> <li>Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen</li> <li>Mitarbeiter befragen</li> <li>Prozesse überprüfen</li> </ul>	<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"> <li>Sicherheit von Containern überprüfen</li> </ul>	<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.
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert und gepflegt?					
12.8.1	Wird eine Liste von Dienstanbietern mit Angabe einer Beschreibung der geleisteten Dienstleistung(en) gepflegt?	<ul style="list-style-type: none"> <li>▪ Richtlinien und Verfahren durchgehen</li> <li>▪ Prozesse überprüfen</li> <li>▪ Liste der Dienstleister überprüfen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	Wird eine schriftliche Vereinbarung aufbewahrt, mit der bestätigt wird, dass der Dienstleister 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.  <i>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.</i>	<ul style="list-style-type: none"> <li>▪ Schriftliche Vereinbarungen überprüfen</li> <li>▪ Richtlinien und Verfahren durchgehen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	Gibt es ein eindeutiges Verfahren für die Inanspruchnahme von Dienstleistern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht?	<ul style="list-style-type: none"> <li>▪ Prozesse überprüfen</li> <li>▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen</li> </ul>	<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.
12.8.4	Gibt es ein Programm zur Überwachung der Dienstleister-Konformität mit dem PCI-Datensicherheitsstandard?	<ul style="list-style-type: none"> <li>▪ Prozesse überprüfen</li> <li>▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen</li> </ul>	<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 Dienstleistern und welche von der Einheit verwaltet werden, aufbewahrt?	<ul style="list-style-type: none"> <li>▪ Prozesse überprüfen</li> <li>▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.1	(a) Wurde ein Vorfalldaktionsplan erstellt, der im Falle einer Systemsicherheitsverletzung im System implementiert wird?	<ul style="list-style-type: none"> <li>▪ Vorfalldaktionsplan überprüfen</li> <li>▪ Verfahren im Zusammenhang mit dem Vorfalldaktionsplan überprüfen</li> </ul>	<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***

Dieser Anhang wird nicht für den SBF B für Händlerbeurteilungen verwendet.

### ***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
<b>1. Einschränkungen</b>	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	
<b>2. Ziel</b>	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
<b>3. Ermitteltes Risiko</b>	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
<b>4. Definition der Kompensationskontrollen</b>	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
<b>5. Validierung der Kompensationskontrollen</b>	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
<b>6. Verwaltung</b>	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 A (Abschnitt 2) mit Datum vom (Abschlussdatum des SBF) notiert wurden.

Auf der Grundlage der Ergebnisse des SBF A 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><b>Konform:</b> Alle Abschnitte des PCI DSS SBF sind vollständig und alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung <b>KONFORM</b>. (Name des Händlerunternehmens) hat somit vollständig Konformität mit dem PCI DSS gezeigt.</p>						
<input type="checkbox"/>	<p><b>Nicht konform:</b> Nicht alle Abschnitte des PCI DSS SBF sind vollständig und/oder nicht alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung <b>NICHT KONFORM</b>. (Name des Händlerunternehmens) hat somit nicht vollständige Konformität mit dem PCI DSS gezeigt.</p> <p><b>Zieldatum</b> 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><b>Konform, jedoch mit gesetzlicher Ausnahme:</b> 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: 30%;">Betroffene Anforderung</th> <th>Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </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 A, 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“) <sup>1</sup> , CAV2-, CVC2-, CID-, CVV2 <sup>2</sup> - oder PIN-Daten <sup>3</sup> 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:	
---	--

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	<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"/>	
12	Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.	<input type="checkbox"/>	<input type="checkbox"/>	

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

