Zahlungskartenbranche (PCI)
Datensicherheitsstandard

Selbstbeurteilungsfragebogen B
und Konformitätsbescheinigung

Nur Prägemaschinen oder eigenständige Terminals mit Dial-Out-Funktion – kein elektronischer Karteninhaberdaten-Speicher

Juni 2018

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 zu den Änderungen am PCI DSS finden Sie unter *PCI DSS – Änderungsübersicht von PCI DSS Version 3.0 auf 3.1*.
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 *PCI DSS – Änderungsübersicht von PCI DSS Version 3.1 auf 3.2.*
Januar 2017	3.2	1.1	Aktualisierte Versionsnummerierung zur Abstimmung mit anderen SBF.
Juni 2018	3.2.1	1.0	Aktualisiert zur Übereinstimmung mit PCI DSS v3.2.1. Ausführliche Informationen zu den Änderungen am PCI DSS finden Sie unter *PCI DSS – Änderungsübersicht von PCI DSS Version 3.2 auf 3.2.1.*

DANKSAGUNG:

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

Inhalt

Vorbereitung

SBF B wurde entwickelt, um die Anforderungen an Händler anzusprechen, die Karteninhaberdaten nur mithilfe von Prägemaschinen oder eigenständigen Terminals mit Dial-Out-Funktion verarbeiten. SBF-B-Händler haben normale Ladengeschäfte (Karte liegt vor) oder sind Post-/Telefonbestellungshändler (Karte liegt nicht vor). Sie speichern keine Karteninhaberdaten in einem Computersystem.

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

- Ihr Unternehmen verwendet ausschließlich eine Prägemaschine und/oder eigenständige Terminals mit Dial-Out-Funktion (über eine Telefonleitung mit Ihrem Prozessor verbunden), um die Zahlungskarteninformationen Ihrer Kunden zu erfassen;
- Die eigenständigen Terminals mit Dial-Out-Funktion sind nicht mit anderen Systemen in Ihrer Umgebung verbunden;
- Die eigenständigen Terminals mit Dial-Out-Funktion sind nicht mit dem Internet verbunden;
- Ihr Unternehmen überträgt keine Karteninhaberdaten über Netzwerke (weder interne Netzwerke noch über das Internet);
- 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:
    - Abschnitt 1 (Teil 1 und 2 der Konformitätsbescheinigung) – Informationen zur Beurteilung und Executive Summary)
    - 2. Abschnitt – PCI-DSS-Selbstbeurteilungsfragebogen (SBF B)
    - 3. Abschnitt (Teil 3 und 4 der Konformitätsbescheinigung) – Validierungs- und Bescheinigungsdetails sowie Aktionsplan für Status „Nicht konform“ (falls zutreffend)

5. Reichen Sie den SBF und die Konformitätsbescheinigung (AOC) zusammen mit allen anderen erforderlichen Dokumenten – zum Beispiel den ASV-Scan-Berichten – beim Acquirer, dem Kartenunternehmen oder einer anderen Anforderungsstelle ein.

Erklärungen zum Selbstbeurteilungsfragebogen

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

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

Dokument	enthält:
PCI DSS *(Anforderungen und Sicherheitsbeurteilungsverfahren des PCI-Datensicherheitsstandards)*	▪ Leitfaden zum Umfang/Geltungsbereich ▪ Leitfaden zum Zweck der PCI-DSS-Anforderungen ▪ Detaillierte Informationen zu Testverfahren ▪ Leitfaden zu Kompensationskontrollen
Anleitung und Richtlinien zum SBF	▪ Informationen zu allen SBF und ihren Qualifikationskriterien ▪ Bestimmung des passenden SBF für Ihr Unternehmen
PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme	▪ Beschreibungen und Definitionen von Begriffen, die im PCI DSS und in den Selbstbeurteilungsfragebögen vorkommen

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

Erwartete Tests

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

Ausfüllen des Selbstbeurteilungsfragebogens

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

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

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

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

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

Gesetzliche Ausnahme

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

1. Abschnitt: Informationen zur Beurteilung

Anleitung zum Einreichen

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

Teil 1. Informationen zum Qualified Security Assessor und Händler

Teil 1a. Händlerinformationen

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

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

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

Teil 2. Zusammenfassung für die Geschäftsleitung

Teil 2a. Handelstätigkeit (alle zutreffenden Optionen auswählen)

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

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

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

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

Teil 2b. Beschreibung des Zahlungskartengeschäfts

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

Teil 2c. Standorte

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

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

Teil 2d. Zahlungsanwendungen

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

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

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

Teil 2e. Beschreibung der Umgebung

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

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

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

Teil 2f. Externe Dienstanbieter

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

Falls ja:

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

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

Teil 2g. Qualifikation zum Ausfüllen des SBF B

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

☐	Der Händler verwendet ausschließlich eine Prägemaschine, um einen Abdruck der Zahlungskarteninformationen des Kunden zu erhalten, und überträgt Karteninhaberdaten weder über eine Telefonleitung noch über das Internet; und/oder Der Händler verwendet ausschließlich eigenständige Dial-Out-Terminals (über eine Telefonleitung mit der Abrechnungsstelle verbunden), welche nicht mit dem Internet oder anderen Systemen in der Händlerumgebung verbunden sind;
☐	Der Händler überträgt keine Karteninhaberdaten über Netzwerke (weder interne Netzwerke noch über das Internet);
☐	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 B

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:

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
3.2	(c) Werden vertrauliche Authentifizierungsdaten nach Abschluss des Autorisierungsprozesses so gelöscht, dass sie nicht wiederhergestellt werden können?	▪ Richtlinien und Verfahren durchgehen. ▪ Systemkonfigurationen untersuchen. ▪ Löschprozesse untersuchen.	☐	☐	☐	☐
	(d) Halten alle Systeme die folgenden Anforderungen hinsichtlich des Verbots ein, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern (auch wenn diese verschlüsselt sind)?					

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
3.2.1	Wird der gesamte Inhalt einer Spur auf dem Magnetstreifen (auf der Rückseite einer Karte, gleichwertige Daten auf einem Chip oder an einer anderen Stelle) nach der Autorisierung nicht gespeichert? *Diese Daten werden auch als Spurdaten, Full-Track-Daten, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet.* ***Hinweis:** Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:* • *Der Name des Karteninhabers,* • *Primäre Kontonummer (PAN),* • *Ablaufdatum und* • *Servicecode* *Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.*	▪ Datenquellen untersuchen, insbesondere: - Eingehende Transaktionsdaten - Sämtliche Protokolle - Verlaufsdateien - Trace-Dateien - Datenbankschema - Datenbankinhalte	☐	☐	☐	☐
3.2.2	Wird der Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte) nach der Autorisierung tatsächlich nicht gespeichert?	▪ Datenquellen untersuchen, insbesondere: - Eingehende Transaktionsdaten - Sämtliche Protokolle - Verlaufsdateien - Trace-Dateien - Datenbankschema - Datenbankinhalte	☐	☐	☐	☐

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

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.
4.2	(b) Sind Richtlinien vorhanden, die festlegen, dass ungeschützte PANs nicht über Messaging-Technologien für Endanwender gesendet werden dürfen?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
7.1	Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten wie folgt ausschließlich auf jene Personen beschränkt, deren Tätigkeit diesen Zugriff erfordert?					
7.1.2	Ist der Zugriff auf privilegierte Benutzer-IDs wie folgt beschränkt? ▪ Auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind ▪ Exklusive Zuweisung zu Rollen, die diesen privilegierten Zugriff konkret benötigen	▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen ▪ Mitarbeiter befragen. ▪ Management befragen. ▪ Privilegierte Benutzer-IDs überprüfen.	☐	☐	☐	☐
7.1.3	Werden Zugriffsberechtigungen anhand der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter zugewiesen?	▪ In Schriftform vorliegende Zugriffskontrollrichtlinien untersuchen ▪ Management befragen. ▪ Benutzer-IDs überprüfen.	☐	☐	☐	☐

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	Wird die physische Sicherheit aller Medien gewährleistet (insbesondere Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)? *Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Medien" auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.*	▪ Richtlinien und Verfahren zur physischen Sicherung von Medien durchgehen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐
9.6	(a) Wird die interne oder externe Verteilung jeglicher Art von Medien stets strikt kontrolliert?	▪ Richtlinien und Verfahren zur Verteilung von Medien durchgehen.	☐	☐	☐	☐
	(b) Umfassen die Kontrollen folgende Punkte?					
9.6.1	Werden Medien klassifiziert, sodass die Sensibilität der Daten bestimmt werden kann?	▪ Richtlinien und Verfahren zur Klassifizierung von Medien durchgehen. ▪ Sicherheitspersonal befragen.	☐	☐	☐	☐
9.6.2	Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?	▪ Mitarbeiter befragen. ▪ Protokolle und Dokumentation zur Verteilung von Medien untersuchen.	☐	☐	☐	☐
9.6.3	Wird vor dem Verlagern von Medien die Genehmigung des Managements eingeholt (insbesondere wenn Medien an Einzelpersonen verteilt werden)?	▪ Mitarbeiter befragen. ▪ Protokolle und Dokumentation zur Verteilung von Medien untersuchen.	☐	☐	☐	☐
9.7	Werden strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durchgeführt?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
9.8	(a) Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen.	☐	☐	☐	☐
	(c) Erfolgt die Vernichtung von Medien wie nachstehend beschrieben?					

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
9.8.1	(a) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen ▪ Mitarbeiter befragen ▪ Prozesse überprüfen	☐	☐	☐	☐
	(b) Werden Container zur Aufbewahrung von zu vernichtenden Informationen so geschützt, dass Zugriffe auf diese Inhalte vermieden werden?	▪ Sicherheit von Containern überprüfen.	☐	☐	☐	☐
9.9	Sind die Geräte, die Zahlungskartendaten über eine direkte physische Interaktion mit der Karte erfassen, vor Manipulation und Austausch geschützt? ***Hinweis:*** *Diese Anforderung gilt für Kartenlesegeräte, die bei Transaktionen eingesetzt werden, bei denen die Karte am Point-of-Sale vorliegt und durch das Gerät gezogen oder in das Gerät eingesteckt werden muss. Diese Anforderung gilt nicht für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke.*					
	(a) Sehen Richtlinien und Verfahren das Führen einer Liste solcher Geräte vor?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
	(b) Sehen Richtlinien und Verfahren vor, dass Geräte regelmäßig auf Manipulations- oder Austauschversuche untersucht werden?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
	(c) Sehen Richtlinien und Verfahren vor, dass das Bewusstsein der Mitarbeiter für verdächtiges Verhalten und das Melden der Manipulation bzw. des Austauschs von Geräten gefördert werden?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐

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? - Fabrikat und Modell des Geräts - Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet) - Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung	▪ Geräteliste überprüfen.	☐	☐	☐	☐
	(b) Ist die Liste korrekt, vollständig und aktuell?	▪ Geräte und Gerätestandorte prüfen und mit der Liste vergleichen.	☐	☐	☐	☐
	(c) Wird die Geräteliste aktualisiert, sobald Geräte hinzugefügt, an einen anderen Standort gebracht, außer Betrieb genommen werden usw.?	▪ Mitarbeiter befragen.	☐	☐	☐	☐
9.9.2	(a) Werden Geräteoberflächen regelmäßig auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch untersucht (stimmen beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht?)? ***Hinweis:*** *Anzeichen für eine Manipulation oder den Austausch von Geräten sind zum Beispiel unerwartete Anbauten oder Kabel, fehlende oder geänderte Sicherheitssiegel, beschädigte oder andersfarbige Gehäuse bzw. Änderungen bei der Seriennummer oder anderen externen Kennzeichen.*	▪ Mitarbeiter befragen. ▪ Untersuchungsprozesse beobachten und mit festgelegten Prozessen vergleichen.	☐	☐	☐	☐
	(b) Kennen die Mitarbeiter die Verfahren zur Untersuchung von Geräten?	▪ Mitarbeiter befragen.	☐	☐	☐	☐

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

Befolgung einer Informationssicherheitsrichtlinie

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

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

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
12.1	Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und an das betroffene Personal weitergeleitet?	▪ Informationssicherheitsrichtlinie überprüfen.	☐	☐	☐	☐
12.1.1	Wird die Sicherheitsrichtlinie mindestens einmal pro Jahr überarbeitet und bei Umgebungsänderungen aktualisiert?	▪ Informationssicherheitsrichtlinie überprüfen. ▪ Verantwortliche Mitarbeiter befragen.	☐	☐	☐	☐
12.3	Wurden Nutzungsrichtlinien für wichtige Technologien entwickelt, um die ordnungsgemäße Nutzung dieser Technologien zu regeln – unter Berücksichtigung der nachfolgenden Punkte? ***Hinweis:*** *Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.*					
12.3.1	Ausdrückliche Genehmigung durch autorisierte Parteien, diese Technologien zu nutzen	▪ Nutzungsrichtlinien überprüfen. ▪ Verantwortliche Mitarbeiter befragen.	☐	☐	☐	☐
12.3.3	Eine Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	▪ Nutzungsrichtlinien überprüfen. ▪ Verantwortliche Mitarbeiter befragen.	☐	☐	☐	☐
12.3.5	Akzeptable Nutzung dieser Technologien	▪ Nutzungsrichtlinien überprüfen. ▪ Verantwortliche Mitarbeiter befragen.	☐	☐	☐	☐
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen. ▪ Per Stichprobe zuständige Mitarbeiter befragen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
12.5	(b) Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?					
12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen.	☐	☐	☐	☐
12.6	(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheitheitsrichtlinien und Verfahren der Karteninhaberdaten zu vermitteln?	▪ Sicherheitsbewusstseinsprogramm durchgehen.	☐	☐	☐	☐
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert und gepflegt?					
12.8.1	Wird eine Liste von Dienstanbietern mit Angabe einer Beschreibung der geleisteten Dienstleistung(en) gepflegt?	▪ Richtlinien und Verfahren durchgehen. ▪ Prozesse überprüfen. ▪ Liste der Dienstanbieter überprüfen.	☐	☐	☐	☐
12.8.2	Wird eine schriftliche Vereinbarung aufbewahrt, mit der bestätigt wird, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden bzw. die er für den Kunden speichert, verarbeitet oder überträgt, oder dass die Sicherheit der CDE betroffen sein könnte. ***Hinweis:*** *Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.*	▪ Schriftliche Vereinbarungen überprüfen. ▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
12.8.3	Gibt es ein eindeutiges Verfahren für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht?	▪ Prozesse überprüfen. ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen.	☐	☐	☐	☐
12.8.4	Gibt es ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard?	▪ Prozesse überprüfen. ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen.	☐	☐	☐	☐
12.8.5	Werden Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden, aufbewahrt?	▪ Prozesse überprüfen. ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen.	☐	☐	☐	☐
12.10.1	(a) Wurde ein Vorfallreaktionsplan erstellt, der im Falle einer Systemsicherheitsverletzung im System implementiert wird?	▪ Vorfallreaktionsplan überprüfen. ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen.	☐	☐	☐	☐

Anhang A: Zusätzliche PCI DSS Anforderungen

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

Dieser Anhang wird nicht für Händlerbeurteilungen verwendet.

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

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

Anhang C: Erläuterung der Nichtanwendbarkeit

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

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

3. Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

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

Aufgrund der obengenannten Ergebnisse des SBF B stellen die in Teil 3b bis 3d angegebenen Unterzeichner den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (Datum) ermittelte Einheit fest (***eine Option angeben):***

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

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

Teil 3a. Feststellung des Status

Unterzeichner bestätigt:

(Zutreffendes ankreuzen)

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

Teil 3. PCI-DSS-Validierung *(Fortsetzung)*

Teil 3a. Feststellung des Status *(Fortsetzung)*

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

Teil 3b. Bescheinigung des Händlers

Unterschrift des Beauftragten des Händlers ↗	*Datum:*
Name des Beauftragten des Händlers:	*Titel:*

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

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

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

Teil 3d. Beteiligung eines ISA (Internal Security Assessor) (sofern zutreffend)

Falls ein ISA an dieser Beurteilung beteiligt war oder dabei geholfen hat, identifizieren Sie bitte den ISA-Mitarbeiter und beschreiben Sie dessen Aufgabe:	

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

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

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

Teil 4. Aktionsplan für Status „Nicht konform“

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

Sprechen Sie sich mit Ihrem Acquirer oder Ihrem/Ihren Kartenunternehmen ab, bevor Sie Teil 4 ausfüllen.

PCI-DSS-Anforderung*	**Anforderungsbeschreibung**	**Konform mit PCI-DSS-Anforderungen** (zutreffende Antwort auswählen)		**Datum bis zur Mängelbeseitigung und Abhilfemaßnahmen** (falls „Nein“ ausgewählt wurde)
		JA	**NEIN**	
3	Schutz gespeicherter Karteninhaberdaten	☐	☐	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	☐	☐	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf	☐	☐	
9	Beschränkung des physischen Zugriffs auf Karteninhaberdaten	☐	☐	
12	Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal	☐	☐	

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