Payment Card Industry
Datensicherheitsstandard

Fragebogen D zur Selbstbewertung für Händler und Bescheinigung der Konformität

Zur Verwendung mit PCI DSS Version 4.0.1

Veröffentlichungsdatum: Oktober 2024

ANMERKUNG: 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.

Dokumentänderungen

Datum	PCI DSS-Version	SAQ Revision	Beschreibung
Oktober 2008	1.2		Um den Inhalt mit den neuen PCI DSS v1.2 zu koordinieren und geringfügige Änderungen zu implementieren, die seit der ursprünglichen v1.1 vermerkt wurden.
Oktober 2010	2.0		Um den Inhalt ist mit den neuen Anforderungen und Testprozeduren von PCI DSS v2.0 zu koordinieren.
Februar 2014	3.0		Um den Inhalt mit den PCI DSS v3.0 Anforderungen und Testprozeduren zu koordinieren und zusätzliche Antwortoptionen einzubeziehen.
April 2015	3.1		Aktualisiert, um mit PCI DSS v3.1 zu koordinieren. Für Details zu PCI DSS-Änderungen, siehe PCI DSS-Zusammenfassung der Änderungen von PCI DSS Version 3.0 zu 3.1.
Juli 2015	3.1	1.1	Aktualisiert, um Verweise auf „bewährte Praktiken“ vor dem 30. Juni 2015 zu entfernen und die PCI DSS v2-Berichtsoption für Anforderung 11.3 zu entfernen.
April 2016	3.2	1.0	Aktualisiert, um mit PCI DSS v3.2 zu koordinieren. Für Details zu PCI DSS-Änderungen, siehe PCI DSS-Zusammenfassung der Änderungen von PCI DSS Version 3.1 zu 3.2.
Januar 2017	3.2	1.1	Aktualisierte Versionsnummerierung, um mit anderen SAQs zu koordinieren.
Juni 2018	3.2.1	1.0	Aktualisiert, um mit PCI DSS v3.2.1 zu koordinieren. Für Details zu PCI DSS-Änderungen, siehe PCI DSS-Zusammenfassung der Änderungen von PCI DSS Version 3.2 zu 3.2.1.
April 2022	4.0		Aktualisiert, um mit PCI DSS v4.0 zu koordinieren. Für Details zu PCI DSS-Änderungen, siehe PCI DSS-Zusammenfassung der Änderungen von PCI DSS Version 3.2.1 zu 4.0. Neu angeordnete, umbenannte und erweiterte Informationen im Abschnitt „Ausfüllen des Fragebogens zur Selbstbewertung“ (zuvor „Bevor Sie beginnen“). Inhalt in den Abschnitten 1 und 3 der Konformitätsbescheinigung (AOC) mit dem PCI DSS v4.0 Bericht zur Konformität AOC koordiniert. Anhänge hinzugefügt, um Antworten auf neue Berichte zu unterstützen.
Dezember 2022	4.0	1	„Vorhanden mit Behebung“ wurde als Berichtsoption aus der Tabelle Anforderungsantworten, Konformitätsbescheinigung (AOC) Teil 2g, SAQ Abschnitt 2 Reaktions-Spalte und AOC Abschnitt 3 entfernt. Ehemaliger Anhang C auch entfernt. „Vorhanden mit CCW“ zu AOC-Abschnitt 3 hinzugefügt. Anleitungen zum Reagieren auf zukünftige Anforderungen hinzugefügt. Kleinere Klarifizierungen hinzugefügt und Tippfehler adressiert.

Oktober 2024	4.0.1		Aktualisiert, um mit PCI DSS v4.0.1 zu koordinieren. Für Details zu PCI DSS-Änderungen, siehe PCI DSS-Zusammenfassung der Änderungen von PCI DSS Version 4.0 zu 4.0.1. Der ASV-Ressourcenleitfaden wurde dem Abschnitt „Zusätzliche PCI SSC-Ressourcen“ hinzugefügt.

Inhalt

Dokumentänderungen ..... **i**
Ausfüllen des Fragebogens zur Selbstbewertung ..... **iv**
Eignungskriterien von Händlern für den Fragebogen D zur Selbstbewertung ..... **iv**
Definition von Kontodaten, Karteninhaberdaten und sensiblen Authentifizierungsdaten ..... **iv**
Fertigstellungsschritte der PCI DSS-Selbstbewertung ..... **v**
Erwartetes Testen ..... **v**
Anforderungsantworten ..... **vi**
Zusätzliche PCI SSC-Ressourcen ..... **ix**
Abschnitt 1: Bewertungsinformationen **1**
Abschnitt 2: Fragebogen D zur Selbstbewertung für Händler **6**
Ein sicheres Netzwerk und sichere Systeme aufbauen und warten **6**
Anforderung 1: Installation und Wartung von Netzwerksicherheitskontrollen *6*
Anforderung 2: Anwendung sicherer Konfigurationen auf alle Systemkomponenten *13*
Schutz von Kontodaten **18**
Anforderung 3: Schutz von gespeicherten Kontodaten *18*
Anforderung 4: Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke *34*
Wartung eines Programms zur Verwaltung von Schwachstellen **37**
Anforderung 5: Schutz aller Systeme und Netzwerke vor bösartiger Software *37*
Anforderung 6: Entwicklung und Wartung sicherer Systeme und Software *42*
Anforderung 7: Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach geschäftlichem Bedarf *56*
Anforderung 8: Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten *61*
Regelmäßige Überwachung und Prüfung der Netzwerke **85**
Anforderung 10: Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten *85*
Anforderung 11: Regelmäßige Prüfung der Sicherheit von Systemen und Netzen *93*
Beibehaltung einer Informationssicherheitspolitik **108**
Anforderung 12: Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme *108*
Anhang A: Zusätzliche PCI DSS-Anforderungen **125**
Anhang A1: Zusätzliche PCI DSS-Anforderungen für Multi-Mandanten-Dienstleistungsanbieter *125*
Anhang A2: Zusätzliche PCI DSS-Anforderungen für Entitäten, die SSL/Early TLS für Karte anwesend POS-POI-Terminalverbindungen verwenden *125*
Anhang A3: Ergänzende Validierung für designierte Entitäten (DESV) *126*
Anhang B: Arbeitsblatt Kompensationssteuerungen **127**
Anhang C: Erklärung der als Nicht Anwendbar vermerkten Anforderungen **128**
Anhang D: Erklärung der als Nicht Getestet vermerkten Anforderungen **129**
Abschnitt 3: Validierungs- und Bescheinigungsdetails **130**

Ausfüllen des Fragebogens zur Selbstbewertung

Eignungskriterien von Händlern für den Fragebogen D zur Selbstbewertung

Der Fragebogen D zur Selbstbewertung (SAQ) D für Händler gilt für Händler, die zum Ausfüllen eines Fragebogens zur Selbsteinschätzung geeignet sind, aber die Kriterien für andere SAQ-Arten nicht erfüllen. Beispiele für Händlerumgebungen, für die SAQ D gelten kann, umfassen, sind aber nicht beschränkt auf:

- E-Commerce-Händler, die Kontodaten auf ihrer Webseite akzeptieren.
- Händler mit elektronischer Speicherung von Kontodaten.
- Händler, die Kontodaten nicht elektronisch speichern, aber die Kriterien einer anderen SAQ-Art nicht erfüllen.
- Händler mit Umgebungen, die möglicherweise die Kriterien einer anderen SAQ-Art erfüllen, für deren Umgebung jedoch zusätzliche PCI DSS-Anforderungen gelten.

Dieser SAQ gilt nicht für Dienstleistungsanbieter.

Definition von Kontodaten, Karteninhaberdaten und sensible Authentifizierungsdaten

PCI DSS richtet sich an alle Entitäten, die Karteninhaberdaten (CHD) und/oder sensible Authentifizierungsdaten (SAD) speichern, verarbeiten oder übertragen oder die Sicherheit der Karteninhaberdaten und/oder sensible Authentifizierungsdaten beeinflussen könnten. Karteninhaberdaten und sensible Authentifizierungsdaten werden als Kontendaten angesehen und sind wie folgt definiert:

Kontodaten	
Karteninhaberdaten beinhalten:	**Sensible Authentifizierungsdaten beinhalten:**
• Primäre Kontonummer (PAN) • Name des Karteninhabers • Ablaufdatum • Dienstleistungskodex	• Vollständige Nachverfolgungsdaten (Magnetstreifendaten oder gleichwertige Daten auf einem Chip) • Kartenverifizierungscode • PINs/PIN-Sperren

Siehe PCI DSS Abschnitt 2, *Informationen zur Anwendbarkeit des PCI DSS*, für weitere Details.

Fertigstellungsschritte der PCI DSS-Selbstbewertung

1. Durch Überprüfung der Eignungskriterien in diesem SAQ und des *Anweisungen und Richtlinien zur Selbstbewertung*-Dokuments auf PCI SSC-Webseite bestätigen, dass dies der richtige SAQ für die Händler-Umgebung ist.
2. Bestätigen, dass die Händler-Umgebung ordnungsgemäß betrachtet ist.
3. Bewerten der Umgebung auf Einhaltung der PCI DSS-Anforderungen.
4. Alle Abschnitte dieses Dokuments ausfüllen:
   - Abschnitt 1: Bewertungsinformationen (Teile 1 und 2 der Konformitätsbescheinigung (AOC) – Kontaktinformationen und ausführliche Zusammenfassung).
   - Abschnitt 2: Fragebogen D zur Selbstbewertung für Händler.
   - Abschnitt 3: Validierungs- und Bescheinigungsdetails (Teile 3 & 4 des AOC – PCI DSS-Validierungs- und Aktionsplans für nicht konforme Anforderungen (wenn Teil 4 anwendbar ist)).
5. Den SAQ und AOC zusammen mit aller anderen angeforderten Dokumentation – wie ASV-Scan-Berichten —an die anfordernde Organisation (die Organisationen, die Konformitäts-Programme wie Zahlungsmarken und Erwerber verwalten).

Erwartetes Testen

Die Anweisungen, die in der Spalte „Erwartetes Testen“ bereitgestellt werden basieren auf den Testprozeduren in PCI DSS und stellen eine allgemeine Beschreibung der Arten von Testaktivitäten bereit, die ein Händler durchführen muss, um zu verifizieren, dass eine Anforderung erfüllt wurde.

Die Absicht hinter jedem Testverfahren wird wie folgt beschrieben:

- Untersuchen: Der Händler beurteilt die Datennachweise kritisch. Übliche Beispiele beinhalten Dokumente (elektronisch oder physisch), Screenshots, Konfigurationsdateien, Audit-Protokolle, und Datendateien.
- Beachten: Der Händler beachtet eine Handlung oder betrachtet etwas in der Umgebung. Beispiele für Beachtungsthemen sind Personal, das Aufgaben oder Prozesse ausführt, Systemkomponenten, die eine Funktion ausführen oder auf Eingaben reagieren, Umgebungsbedingungen und physische Kontrollen.
- Interview: Der Händler führt Gespräche mit einzelnen Mitarbeitern. Interview-Zielsetzungen können die Bestätigung sein, ob eine Aktivität durchgeführt wird, Beschreibungen, wie eine Aktivität durchgeführt wird und ob das Personal über besondere Kenntnisse oder Verstehen verfügt.

Die Testmethoden sollen es dem Händler ermöglichen, zu demonstrieren, wie er eine Anforderung erfüllt hat. Die zu untersuchenden oder zu beobachtenden spezifischen Punkte und das zu befragende Personal sollten sowohl für die zu bewertende Anforderung als auch für die jeweilige Umsetzung des Händlers geeignet sein.

Vollständige Details von Testprozeduren für jede Anforderung kann im PCI DSS gefunden werden.

Anforderungsantworten

Für jedes Anforderungselement gibt es eine Auswahl an Antworten, um den Status des Händlers in Bezug auf diese Anforderung anzugeben. ***Für jedes Anforderungselement sollte nur eine Reaktion ausgewählt werden.***

Eine Beschreibung der Bedeutung jeder Reaktion wird in der folgenden Tabelle bereitgestellt:

Antwort	Wann diese Reaktion verwendet werden soll:
Vorhanden	Das erwartete Testen wurde durchgeführt und alle Elemente der Anforderung wurden wie angegeben erfüllt.
Vorhanden mit CCW (Arbeitsblatt Kompensationssteuerungen)	Das erwartete Testen wurde durchgeführt und die Anforderung wurde mit Hilfe einer kompensierenden Kontrolle erfüllt. Alle Antworten in dieser Spalte erfordern das Ausfüllen eines Arbeitsblatts für Kompensationskontrollen (CCW) in Anhang B von diesem SAQ. Informationen zur Benutzung von Kompensationskontrollen und Anleitungen zum Ausfüllen des Arbeitsblatts wird in den Anhängen B und C des PCI DSS bereitgestellt.
Nicht Anwendbar	Die Anforderung gilt nicht für die Umgebung des Händlers. (Beispiele siehe „Leitfaden für Nicht Anwendbar Anforderungen“ unten.)Alle Antworten in dieser Spalte erfordern eine unterstützende Erklärung in Anhang C von diesem SAQ.
Nicht Getestet	Die Anforderung wurde nicht in die Bewertung eingeschlossen und in keiner Weise getestet. (Siehe „Verstehen des Unterschieds zwischen Nicht Anwendbar und Nicht Getestet” unten für Beispiele, wann diese Option verwendet werden sollte.) Alle Antworten in dieser Spalte erfordern eine unterstützende Erklärung in Anhang D von diesem SAQ.
Nicht Vorhanden	Einige oder alle Elemente der Anforderung wurden nicht erfüllt oder werden derzeit implementiert oder erfordern weitere Tests, bevor der Händler bestätigen kann, dass sie vorhanden sind. Die Antworten in dieser Spalte erfordern möglicherweise das Ausfüllen von Teil 4, wenn dies von der Entität angefordert wird, an die dieser SAQ übermittelt wird. Diese Antwort wird auch verwendet, wenn eine Anforderung aufgrund einer gesetzlichen Einschränkung nicht erfüllt werden kann. (Siehe „Legale Ausnahme“ unten für weitere Anleitungen).

Anleitungen für nicht anwendbare Anforderungen

Während viele Händler, die SAQ D ausfüllen, die Konformität mit allen PCI DSS-Anforderungen validieren müssen, stellen einige Entitäten mit sehr spezifischen Geschäftsmodellen möglicherweise fest, dass einige Anforderungen nicht gelten. Zum Beispiel wird von Entitäten, die in keiner Weise drahtlose Technologie verwenden, nicht erwartet, dass sie die PCI DSS-Anforderungen erfüllen, die spezifisch für die Verwaltung drahtloser Technologie sind. Ebenso wird von Entitäten, die zu keinem Zeitpunkt Kontodaten elektronisch speichern, nicht erwartet, dass sie die PCI DSS-Anforderungen in Bezug auf die sichere Speicherung von Kontodaten erfüllen (zum Beispiel Anforderung 3.5.1). Ein weiteres Beispiel sind Anforderungen spezifisch für die Anwendungsentwicklung und sichere Codierung (zum Beispiel Anforderungen 6.2.1 bis 6.2.4), die nur für eine Entität mit maßgeschneiderter Software gelten (von einem Drittanbieter gemäß den Spezifikationen der Entität für die Entität entwickelt) oder kundenspezifische Software (von der Entität für den eigenen Gebrauch entwickelt).

Für jede Antwort, bei der in diesem SAQ „Nicht Anwendbar“ ausgewählt ist, Anhang C ausfüllen: Erklärung der als Nicht Anwendbar vermerkten Anforderungen.

Verstehen des Unterschieds zwischen Nicht Anwendbar und Nicht Getestet

Anforderungen, die auf eine Umgebung als nicht anwendbar erachtet werden, müssen als solche verifiziert werden. Mit Verwendung des drahtlosen Beispiels oben, muss ein Händler, damit er „Nicht Anwendbar“ für die Anforderungen 1.3.3, 2.3.1, 2.3.2 und 4.2.1.2 auswählen kann, zunächst bestätigen, dass in seiner Karteninhaberdaten-Umgebung (CDE) keine drahtlosen Technologien verwendet werden oder die sich mit ihrer CDE verbinden. Sobald dies bestätigt wurde, kann der Händler für diese spezifischen Anforderungen „Nicht Anwendbar“ auswählen.

Wenn eine Anforderung ohne Prüfung, ob sie zutreffen *könnte*, vollständig von der Überprüfung ausgeschlossen wird, sollte die Option „Nicht Getestet“ ausgewählt werden. Beispiele für Situationen, in denen dies auftreten könnte, könnten umfassen:

- Ein Händler wird von seinem Erwerber gebeten, eine Teilmenge von Anforderungen zu validieren – zum Beispiel mit Verwendung des PCI DSS-priorisierten Ansatzes, um nur bestimmte Meilensteine zu validieren.

Ein Händler bestätigt eine neue Sicherheitskontrolle, die sich nur auf einen Teil der Anforderungen auswirkt – zum Beispiel die Implementierung einer neuen Verschlüsselungsmethodik, die nur die Bewertung der PCI DSS-Anforderungen 2, 3 und 4 erfordert. In diesen Szenarien umfasst die Bewertung des Händlers nur bestimmte PCI DSS-Anforderungen, obwohl möglicherweise auch andere Anforderungen für seine Umgebung gelten.

Wenn irgendwelche Anforderungen vollständig von der Selbstbewertung des Händlers ausgeschlossen sind, für diese spezifische Anforderung Nicht Getestet auswählen und Anhang D ausfüllen: Erklärung der Nicht Getesteten Anforderungen für jeden „Nicht Getestet“-Eintrag. Eine Bewertung mit Nicht Getestet Antworten ist eine „partielle“ PCI DSS-Bewertung und wird als solche vom Händler in der Konformitätsbescheinigung in Abschnitt 3, Teil 3 von diesem SAQ vermerkt.

Anleitungen zum Reagieren auf zukünftige Anforderungen hinzugefügt

In Abschnitt 2 unten enthält jede PCI DS-Anforderung oder jeder Aufzählungspunkt mit einem verlängerten Implementierungszeitraum den folgenden Hinweis: „*Diese Anforderung [oder Aufzählungspunkt] ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*"

Diese neuen Anforderungen müssen erst nach Ablauf des zukünftigen Datums in eine PCI DSS-Bewertung aufgenommen werden. Vor diesem zukünftigen Datum können alle Anforderungen mit einem verlängerten Implementierungsdatum, die vom Händler nicht implementiert wurden, als „Nicht Anwendbar" gekennzeichnet und *in Anhang C dokumentiert werden: Erklärung der als Nicht Anwendbar vermerkten Anforderungen*.

Legale Ausnahme

Wenn Ihre Organisation einer legalen Beschränkung unterliegt, die die Organisation daran hindert, eine PCI DSS-Anforderung zu erfüllen, für diese Anforderung Nicht Vorhanden auswählen und die entsprechende Bescheinigung in Abschnitt 3, Teil 3 dieses SAQ ausfüllen.

Hinweis: *Eine gesetzliche Ausnahme ist eine rechtliche Einschränkung aufgrund eines lokalen oder regionalen Gesetzes, einer Verordnung oder einer behördlichen Vorschrift, wenn die Erfüllung einer PCI DSS-Anforderung gegen dieses Gesetz, diese Verordnung oder diese behördliche Vorschrift verstoßen würde.*

Vertragliche Verpflichtungen oder Rechtsberatung sind keine legalen Beschränkungen.

Verwendung des kundenspezifischen Ansatzes

Verwendung des kundenspezifischen Ansatzes wird in SAQs nicht unterstützt.

SAQs können nicht verwendet werden, um die Verwendung des kundenspezifischen Ansatzes zu dokumentieren, um die PCI DSS-Anforderungen zu erfüllen. Aus diesem Grund sind die Zielsetzungen des kundenspezifischen Ansatzes nicht in SAQs enthalten. Entitäten, die mit Verwendung des kundenspezifischen Ansatzes validieren möchten, können möglicherweise die Vorlage für den PCI-DSS Konformitätsbericht (ROC) verwenden, um die Ergebnisse ihrer Bewertung zu dokumentieren.

Die Verwendung des kundenspezifischen Ansatzes kann von Organisationen reguliert werden, die Einhaltungsprogramme verwalten, wie Zahlungsmarken und Erwerber. Fragen über die Verwendung eines kundenspezifischen Ansatzes sollten immer an diese Organisationen verwiesen werden. Dazu gehört, ob eine Entität, die für einen SAQ geeignet ist, stattdessen einen ROC ausfüllen kann, um einen kundenspezifischen Ansatz zu verwenden, und ob eine Entität einen QSA verwenden muss oder einen ISA verwenden kann, um eine Bewertung mit Verwendung des kundenspezifischen Ansatzes durchzuführen. Informationen zur Verwendung des kundenspezifischen Ansatzes kann in Anhang D und E des PCI DSS gefunden werden.

Zusätzliche PCI SSC-Ressourcen

Zusätzliche Ressourcen, die Anleitungen zu den PCI DSS-Anforderungen bereitstellen und wie der Fragebogen zur Selbstbewertung ausgefüllt wird, wurden unten bereitgestellt, um beim Bewertungsprozess zu helfen.

Ressource	Beinhaltet:
PCI Datensicherheitsstandard-Anforderungen und Testprozeduren (PCI DSS)	▪ Anleitungen zum Scoping ▪ Anleitungen zur Absicht aller PCI DSS-Anforderungen ▪ Details von Testprozeduren ▪ Anleitungen zu kompensierenden Kontrollen ▪ Anhang G: Glossar der Begriffe, Abkürzungen und Akronyme
SAQ Anweisungen und Anleitungen	▪ Informationen über alle SAQs und ihren Eignungskriterien ▪ Wie bestimmt wird, welcher SAQ der richtige für Ihre Organisation ist
Häufig gestellte Fragen (FAQs)	▪ Anleitungen und Informationen über SAQs.
Online PCI DSS Glossar	▪ PCI DSS Begriffe, Abkürzungen und Akronyme
Ergänzende Informationen und Richtlinien	▪ Anleitungen zu einer Vielzahl von PCI DSS-Themen, einschließlich: – *Verstehen von PCI DSS-Scoping und Netzwerksegmentierung.* – *Sicherheitsgarantie von Drittanbietern* – *Anleitungen zur Multi-Faktor-Authentifizierung* – *Bewährte Praktiken zur Aufrechterhaltung der PCI-DSS-Konformität*
Mit PCI beginnen	▪ Ressourcen für kleinere Händler einschließlich: – *Leitfaden für sicheren Zahlungsverkehr* – *Gängige Zahlungssysteme* – *Fragen, die Sie Ihren Anbietern stellen sollen* – *Glossar von Zahlungs- und Informationssicherheitsbegriffen* – *PCI Firewall-Grundlagen* – *ASV-Ressourcenleitfaden*

Diese und andere Ressourcen können auf der PCI SSC-Webseite *(www.pcisecuritystandards.org)* gefunden werden.

Organisationen werden ermutigt, PCI DSS und andere unterstützende Dokumente zu lesen, bevor sie mit einer Bewertung beginnen.

Abschnitt 1: Bewertungsinformationen

Anweisungen zur Einreichung

Dieses Dokument muss als Erklärung der Ergebnisse der Selbstbewertung des Händlers anhand der *Payment Card Industry- Datensicherheitsstandards (PCI DSS)-Anforderungen und Testprozeduren* ausgefüllt werden. Alle Abschnitte ausfüllen. Der Händler ist verantwortlich, sicherzustellen, dass jeder Abschnitt, soweit zutreffend, von den entsprechenden Parteien ausgefüllt wird. Kontaktieren der Entität(en) an die die Konformitätsbescheinigung (AOC) übermittelt wird(werden), um Informationen zu den Berichts- und Übermittlungsprozeduren zu erhalten.

Teil 1. Kontaktinformationen

Teil 1a. Bewerteter Händler

Unternehmensname:	
DBA (handelnd als):	
Postanschrift des Unternehmens:	
Hauptwebseite des Unternehmens:	
Kontaktname des Unternehmens:	
Kontakttitel des Unternehmens:	
Kontakt-Telefonnummer:	
Kontakt-E-Mailadresse:	

Teil 1b. Bewerter

Bereitstellen der folgenden Informationen für alle an der Bewertung beteiligten Bewerter. Wenn es für eine bestimmten Bewerterart keinen Bewerter gab, Nicht Anwendbar eingeben.

PCI SSC-Interne Sicherheitsbewerter	
ISA-Name(n):	
Qualifizierter Sicherheitsbewerter	
Unternehmensname:	
Postanschrift des Unternehmens:	
Webseite des Unternehmens:	
Name des Hauptbewerters:	
Telefonnummer des Bewerters:	
E-Mailadresse des Bewerters:	
Zertifikatsnummer des Bewerters:	

Teil 2. Ausführliche Zusammenfassung

Teil 2a. Zahlungskanäle für Händlerfirmen (alle geltenden auswählen):

Angeben aller von der Firma verwendeten Zahlungskanäle, die in dieser Bewertung enthalten sind.

☐ Versandbestellung/Telefonbestellung (MOTO)

☐ E-Commerce

☐ Karte vorhanden

Sind irgendwelche Zahlungskanäle in dieser Bewertung nicht enthalten? Wenn ja, Angeben, welche(r) Kanal(e) nicht in der Bewertung enthalten ist (sind) und Bereitstellen einer kurzen Erklärung, warum der Kanal ausgeschlossen wurde.	☐ Ja ☐ Nein

Hinweis: *Wenn die Organisation einen Zahlungskanal hat, der nicht von diesem SAQ abgedeckt wird, konsultieren der Entität(en) bezüglich der Validierung für die anderen Kanäle, an die diese AOC übermittelt wird.*

Teil 2b. Beschreibung der Rolle mit Zahlungskarten

Für jeden Zahlungskanal, der in dieser Bewertung enthalten ist, wie oben in Teil 2a ausgewählt, beschreiben, wie das Unternehmen Kontodaten speichert, verarbeitet und/oder sendet.

Kanal	Wie die Firma Kontodaten speichert, verarbeitet und/oder überträgt

Teil 2c. Beschreibung der Zahlungskartenumgebung

Bereitstellen einer ***hochrangigen*** Beschreibung der Umgebung, die von dieser Bewertung abgedeckt wird. *Zum Beispiel:* • *Verbindungen in und aus der Karteninhaberdatenumgebung (CDE).* • *Kritische Systemkomponenten innerhalb der CDE, wie z. B. POI-Geräte, Datenbanken, Webserver usw., und ggf. alle anderen erforderlichen Zahlungskomponenten.* • *Systemkomponenten, die die Sicherheit der Kontodaten beeinträchtigen könnten.*	
Angeben, ob die Umgebung eine Segmentierung enthält, um den Geltungsbereich der Bewertung zu verringern. *(Siehe den Abschnitt „Segmentierung“ von PCI DSS zu Anleitungen zur Segmentierung.)*	☐ Ja ☐ Nein

Teil 2. Ausführliche Zusammenfassung *(fortgesetzt)*

Teil 2d. Standorte/Einrichtungen im Geltungsbereich

Auflisten aller Arten von physischen Standorten/Einrichtungen (zum Beispiel Einzelhandelsstandorte, Firmenbüros, Rechenzentren, Callcenter und Poststellen) im Geltungsbereich der PCI DSS-Bewertung.

Einrichtungsart	**Gesamtzahl von Standorten** (Wie viele Standorte dieser Art im Geltungsbereich sind)	**Standort(e) der Einrichtung (Stadt, Land)**
Beispiel: Datenzentren	*3*	*Boston, MA, USA*

Teil 2e. PCI SSC-Validierte Produkte und Lösungen

Verwendet der Händler irgendeinen Artikel, der auf einer PCI SSC-Liste von validierten Produkten und Lösungen* identifiziert ist♦?

☐ Ja ☐ Nein

Bereitstellen der folgenden Informationen zu jedem Artikel an, das der Händler aus den Listen validierter Produkte und Lösungen von PCI SSC verwendet:

Name des PCI SSC-validierten Produkts oder Lösung	**Version des Produkts oder der Lösung**	**PCI SSC-Standard, nach dem das Produkt oder die Lösung validiert wurde**	**PCI SSC-Listen-Referenznummer**	**Ablaufdatum der Auflistung** (TT-MM-JJJJ)
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ
				TT-MM-JJJJ

♦ Zwecke dieses Dokuments bedeutet „Liste validierter Produkte und Lösungen“ die Listen validierter Produkte, Lösungen und/oder Komponenten, die auf der PCI SSC-Webseite (www.pcisecuritystandards.org) — erscheinen zum Beispiel 3DS Software-Entwicklungs-Kits, Genehmigte PTS-Geräte, validierte Zahlungssoftware, Punkt-zu-Punkt-Verschlüsselungslösungen (P2PE), softwarebasierte PIN-Eingabe auf COTS-Lösungen (SPoC) und kontaktlose Zahlungen auf COTS-Lösungen (CPoC) und mobile Zahlung auf COTS-Produkten (MPoC).

Teil 2. Ausführliche Zusammenfassung *(fortgesetzt)*

Teil 2f. Drittanbieter von Dienstleistungen

Unterhält der Händler Beziehungen zu einem oder mehreren Drittanbietern von Dienstleistungen, die:

• Kontodaten im Auftrag des Händlers speichern, verarbeiten oder übertragen (zum Beispiel Zahlungs-Gateways, Zahlungsabwickler, Zahlungsdienstleistungsanbieter (PSPs), und externe Speicherung)	☐ Ja ☐ Nein
• Systemkomponenten, die in dem Geltungsbereich der PCI DSS-Bewertung--des Händler sind, verwalten, zum Beispiel über Anbieter von Netzwerksicherheitskontrolldienstleistungen, Anti-Malware-Dienstleistungen und Verwaltung von Sicherheitsvorfällen und Ereignissen (SIEM); Kontakt- und Callcenter, Webhosting-Dienstleistungen, und IaaS, PaaS, SaaS- und FaaS-Cloud-Anbieter.	☐ Ja ☐ Nein
• Die Sicherheit der CDE des Händlers beeinträchtigen könnten (zum Beispiel Anbieter, die Unterstützung per Fernzugriff bereitstellen, und/oder Entwickler von maßgeschneiderter Software).	☐ Ja ☐ Nein

Wenn Ja:

Name des Dienstleistungsanbieters:	**Beschreibung der bereitgestellten Dienstleistung(en):**

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

Teil 2. Ausführliche Zusammenfassung *(fortgesetzt)*

Teil 2g. Zusammenfassung der Bewertung

(SAQ Abschnitt 2 und verwandte Anhänge)

Unten alle Antworten angeben, die für jede PCI-DSS-Anforderung ausgewählt wurden.

PCI DSS-Anforderung	Anforderungsantworten *Für eine gegebene Anforderung kann mehr als eine Antwort ausgewählt werden. Alle zutreffenden Antworten angeben.*				
	Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
Anforderung 1:	☐	☐	☐	☐	☐
Anforderung 2:	☐	☐	☐	☐	☐
Anforderung 3:	☐	☐	☐	☐	☐
Anforderung 4:	☐	☐	☐	☐	☐
Anforderung 5:	☐	☐	☐	☐	☐
Anforderung 6:	☐	☐	☐	☐	☐
Anforderung 7:	☐	☐	☐	☐	☐
Anforderung 8:	☐	☐	☐	☐	☐
Anforderung 9:	☐	☐	☐	☐	☐
Anforderung 10:	☐	☐	☐	☐	☐
Anforderung 11:	☐	☐	☐	☐	☐
Anforderung 12:	☐	☐	☐	☐	☐
Anhang A2:	☐	☐	☐	☐	☐

Abschnitt 2: Fragebogen D zur Selbstbewertung für Händler

Hinweis: *Die folgenden Anforderungen spiegeln die Anforderungen* im *Dokument* PCI-DSS-Anforderungen und Testverfahren *wider*.

Fertigstellungsdatum der Selbstbewertung: TT-MM-JJJJ

Ein sicheres Netzwerk und sichere Systeme aufbauen und warten

Anforderung 1: Installation und Wartung von Netzwerksicherheitskontrollen

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.1 Prozesse und Mechanismen zur Installation und Wartung von Netzwerksicherheitskontrollen werden definiert und verstanden.							
1.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 1 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
1.1.2	Die Rollen und Zuständigkeiten für die Durchführung der Aktivitäten gemäß Anforderung 1 sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
1.2 Netzwerksicherheitskontrollen (NSCs) werden konfiguriert und gewartet.							
1.2.1	Konfigurationsstandards für NSC-Regelsätze sind: • Definiert. • Implementiert. • Gewartet.	• Konfigurationsstandards untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.2.2	Alle Änderungen an Netzwerkverbindungen und an Konfigurationen von NSCs werden gemäß dem in Anforderung 6.5.1 definierten Änderungskontrollprozess genehmigt und verwaltet.	• Dokumentierte Prozeduren untersuchen. • Netzwerkkonfigurationen untersuchen. • Änderungskontrollaufzeichnungen untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Änderungen an Netzwerkverbindungen beinhalten das Hinzufügen, Entfernen oder Ändern einer Verbindung. Änderungen an NSC-Konfigurationen beinhalten solche, die sich auf die Komponente selbst beziehen, sowie solche, die sich darauf auswirken, wie sie ihre Sicherheitsfunktion ausführt.						
1.2.3	Genaue Netzwerkdiagramme werden beibehalten, die alle Verbindungen zwischen der CDE und anderen Netzwerken, einschließlich aller drahtlosen Netzwerke, zeigen.	• Netzwerkdiagramme untersuchen. • Netzwerkkonfigurationen untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Ein aktuelles Netzwerkdiagramm oder eine andere technische oder topologische Lösung, die die Netzwerkverbindungen und -geräte identifiziert, kann zur Erfüllung dieser Anforderung verwendet werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.2.4	Genaue Datenflussdiagramm(e) werden gewartet, die Folgendes erfüllen: • Zeigt alle Kontodatenflüsse über Systeme und Netzwerke an. • Wird bei Änderungen an der Umgebung nach Bedarf aktualisiert.	• Datenflussdiagramme untersuchen. • Netzwerkkonfigurationen beachten. • Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Ein Datenflussdiagramm(e) oder eine andere technische oder topologische Lösung, die Flüsse von Kontodaten über Systeme und Netzwerke identifiziert, kann zur Erfüllung dieser Anforderung verwendet werden.						
1.2.5	Alle zulässigen Dienstleistungen, Protokolle und Ports werden identifiziert, genehmigt und haben einen definierten Geschäftsbedarf.	• Dokumentation untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
1.2.6	Für alle Dienstleistungen, Protokolle und Ports, die verwendet werden und als unsicher gelten, werden Sicherheitsfunktionen definiert und implementiert, sodass das Risiko gemindert wird.	• Dokumentation untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
1.2.7	Konfigurationen von NSCs werden mindestens alle sechs Monate überprüft, um zu bestätigen, dass sie relevant und effektiv sind.	• Dokumentierte Prozeduren untersuchen. • Dokumentation von durchgeführten Überprüfungen untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.2.8	Konfigurationsdateien für NSCs sind: • Vor nicht autorisiertem Zugriff gesichert. • Werden konsistent mit aktiven Netzwerkkonfigurationen gehalten.	• NSC-Konfigurationsdateien untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Jede Datei oder Einstellung, die zum Konfigurieren oder Synchronisieren von NSCs verwendet wird, wird als „Konfigurationsdatei“ betrachtet. Dies beinhaltet Dateien, automatisierte und systembasierte Kontrollen, Skripte, Einstellungen, Infrastruktur als Code oder andere Parameter, die gesichert, archiviert oder entfernt gespeichert werden.						
1.3 Der Netzwerkzugriff auf und von der Karteninhaberdatenumgebung ist eingeschränkt.							
1.3.1	Der eingehende Verkehr zur CDE wird wie folgt eingeschränkt: • Nur auf Verkehr, der notwendig ist, • Jeder andere Verkehr wird gezielt verweigert.	• NSC-Konfigurationsstandards untersuchen. • NSC-Konfigurationen untersuchen.	☐	☐	☐	☐	☐
1.3.2	Der ausgehende Verkehr von der CDE wird wie folgt eingeschränkt: • Nur auf Verkehr, der notwendig ist. • Jeder andere Verkehr wird gezielt verweigert.	• NSC-Konfigurationsstandards untersuchen. • NSC-Konfigurationen untersuchen.	☐	☐	☐	☐	☐
1.3.3	NSCs werden zwischen allen drahtlosen Netzwerken und der CDE installiert, unabhängig davon, ob es sich bei dem drahtlosen Netzwerk um ein CDE handelt, so dass: • Der gesamte drahtlose Verkehr von drahtlosen Netzwerken in die CDE wird standardmäßig abgelehnt. • Nur drahtloser Verkehr mit einem autorisierten Geschäftszweck ist in die CDE zugelassen.	• Konfigurationseinstellungen untersuchen. • Netzwerkdiagramme untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.4 Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert.							
1.4.1	NSCs werden zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken implementiert.	• NSC-Konfigurationsstandards untersuchen. • Aktuelle Netzwerkdiagramme untersuchen. • Netzwerkkonfigurationen untersuchen.	☐	☐	☐	☐	☐
1.4.2	Eingehender Verkehr von nicht vertrauenswürdigen Netzwerken zu vertrauenswürdigen Netzwerken ist beschränkt auf: • Kommunikationen mit Systemkomponenten, die autorisiert sind, öffentlich zugängliche Dienste, Protokolle und Ports bereitzustellen. • Zustandsbehaftete Antworten auf Kommunikationen, die von Systemkomponenten in einem vertrauenswürdigen Netzwerk eingeleitet wurden. • Alle anderen Verkehre werden verweigert.	• NSC-Dokumentation untersuchen. • NSC-Konfigurationen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Die Absicht dieser Anforderung besteht darin, Kommunikationssitzungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken zu adressieren, anstatt die Besonderheiten von Protokollen. Diese Anforderung schränkt die Verwendung von UDP oder anderen verbindungslosen Netzwerkprotokollen nicht ein, wenn der Zustand vom NSC aufrechterhalten wird.						
1.4.3	Anti-Spoofing-Maßnahmen werden implementiert, um gefälschte Quell-IP-Adressen zu erkennen und daran zu hindern, in das vertrauenswürdige Netzwerk einzudringen.	• NSC-Dokumentation untersuchen. • NSC-Konfigurationen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.4.4	Auf Systemkomponenten, die Karteninhaberdaten speichern, kann von nicht vertrauenswürdigen Netzwerken nicht direkt zugegriffen werden.	• Datenflussdiagramm und Netzwerkdiagramm untersuchen. • NSC-Konfigurationen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt nicht für die Speicherung von Kontodaten in flüchtigem Speicher, gilt jedoch dort, wo der Speicher als persistenter Speicher behandelt wird (z. B. RAM-Disk). Kontodaten können nur während der Zeit im flüchtigen Speicher gespeichert werden, die zur Unterstützung des zugehörigen Geschäftsprozesses erforderlich ist (zum Beispiel bis zum Abschluss der entsprechenden Zahlungskartentransaktion).						
1.4.5	Die Offenlegung interner IP-Adressen und Routing-Informationen ist nur auf autorisierten Parteien beschränkt.	• NSC-Konfigurationen untersuchen. • Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung	Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
		Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
1.5 Risiken für die CDE durch Computergeräte, die sich sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbinden können, werden gemindert.						
1.5.1	Sicherheitskontrollen werden auf allen Computergeräten implementiert, einschließlich unternehmens- und mitarbeitereigenen Geräten, die sich mit nicht vertrauenswürdigen Netzwerken (einschließlich dem Internet) und der CDE wie folgt verbinden: • Spezifische Konfigurationseinstellungen werden definiert, um zu verhindern, dass Bedrohungen in das Netzwerk der Entität eingeführt werden. • Sicherheitskontrollen werden aktiv durchgeführt. • Sicherheitskontrollen können von Benutzern der Computergeräte nicht geändert werden, es sei denn, dies wird von der Geschäftsleitung im Einzelfall für einen begrenzten Zeitraum ausdrücklich dokumentiert und genehmigt.	• Richtlinien und Konfigurationsstandards untersuchen. • Gerätekonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Sicherheitskontrollen dürfen nur dann vorübergehend deaktiviert werden, wenn ein berechtigter technischer Bedarf besteht, der von der Verwaltung im Einzelfall genehmigt wird. Wenn diese Sicherheitskontrollen für einen bestimmten Zweck deaktiviert werden müssen, muss dieses formell autorisiert werden. Für den Zeitraum, in dem diese Sicherheitskontrollen nicht aktiv sind, müssen möglicherweise zusätzliche Sicherheitsmaßnahmen implementiert werden. Diese Anforderung gilt für mitarbeiter- und unternehmenseigene Computergeräte. Systeme, die nicht durch Unternehmensrichtlinien verwaltet werden können, führen zu Schwachstellen und stellen Möglichkeiten bereit, die böswillige Personen ausnutzen können.						

Anforderung 2: Anwendung sicherer Konfigurationen auf alle Systemkomponenten

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
2.1 Prozesse und Mechanismen zum Anwenden sicherer Konfigurationen auf alle Systemkomponenten werden definiert und verstanden.							
2.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 2 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
2.1.2	Die Rollen und Verantwortlichkeiten für die Durchführung der in Anforderung 2 genannten Tätigkeiten sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
2.2 Systemkomponenten werden sicher konfiguriert und verwaltet.							
2.2.1	Konfigurationsstandards werden entwickelt, implementiert und gewartet, um: • Alle Systemkomponenten abzudecken. • Alle bekannten Schwachstellen zu adressieren. • Mit branchenübliche Standards für die Systemhärtung oder die Empfehlungen der Anbieter zur Härtung konsistent zu sein. • Wenn neue Schwachstellen identifiziert werden, wie in Anforderung 6.3.1 definiert, aktualisiert zu sein. • Wenn neue Systeme konfiguriert und verifiziert werden, wie sie bevor oder unmittelbar vorhanden sind, nachdem eine Systemkomponente mit einer Produktionsumgebung verbunden wird, angewandt zu sein.	• Systemkonfigurationsstandards untersuchen. • Die branchenweit akzeptierten Härtungsstandards überprüfen. • Konfigurationseinstellungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
2.2.2	Anbieter-Standardkonten werden wie folgt verwaltet: • Wenn die Anbieter-Standardkonten verwendet werden, wird das Standardpasswort gemäß Anforderung 8.3.6 geändert. • Wenn die Anbieter-Standardkonten nicht verwendet werden, wird das Konto entfernt oder deaktiviert.	• Systemkonfigurationsstandards untersuchen. • Anbieterdokumentation untersuchen. • Beachten, wie sich ein Systemadministrator mit den Standardkonten des Anbieters anmeldet. • Konfigurationsdateien untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Dies gilt für ALLE Anbieter-Standardkonten und -Passwörter, einschließlich, aber nicht beschränkt auf diejenigen, die von Betriebssystemen verwendet werden, Software, die Sicherheitsdienstleistungen bereitstellt, Anwendungs- und Systemkonten, Verkaufsstellen-Terminals (POS), Zahlungsanwendungen und Simple Network Standardeinstellungen für das einfache Netzwerkverwaltungsprotokoll (SNMP). Diese Anforderung gilt auch, wenn eine Systemkomponente nicht in der Umgebung einer Entität installiert ist, zum Beispiel Software und Anwendungen, die Teil der CDE sind und auf die über eine Cloud-Abonnementdienstleistung zugegriffen wird.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
2.2.3	Primäre Funktionen, die unterschiedliche Sicherheitsstufen erfordern, werden wie folgt verwaltet: • Auf einer Systemkomponente existiert nur eine primäre Funktion, **ODER** • Primäre Funktionen mit unterschiedlichen Sicherheitsstufen, die auf derselben Systemkomponente existieren, sind voneinander isoliert, **ODER** • Primäre Funktionen mit unterschiedlichen Sicherheitsstufen auf derselben Systemkomponente werden alle auf der Stufe gesichert, die die Funktion mit dem höchsten Sicherheitsbedürfnis erfordert.	• Systemkonfigurationsstandards untersuchen. • Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐
2.2.4	Nur notwendige Dienstleistungen, Protokolle, Dämonen und Funktionen werden aktiviert und jede unnötige Funktionalität wird entfernt oder deaktiviert.	• Systemkonfigurationsstandards untersuchen. • Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐
2.2.5	Wenn irgendwelche unsicheren Dienstleistungen, Protokolle oder Dämonen vorhanden sind: • Die geschäftliche Rechtfertigung wird dokumentiert. • Zusätzliche Sicherheitsfunktionen werden dokumentiert und implementiert, die das Risiko der Verwendung unsicherer Dienstleistungen, Protokollen oder Dämonen reduzieren.	• Konfigurationsstandards untersuchen. • Personal befragen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
2.2.6	Systemsicherheitsparameter werden konfiguriert, um Missbrauch zu verhindern.	• Systemkonfigurationsstandards untersuchen. • Personal befragen. • Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
2.2.7	Alle administrativen Nicht-Konsolen-Zugriffe werden mit Verwendung von starker Kryptographie verschlüsselt.	• Systemkonfigurationsstandards untersuchen. • Eine Administratoranmeldung beachten. • Systemkonfigurationen untersuchen. • Anbieterdokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Dies beinhaltet den administrativen Zugriff über browserbasierte Schnittstellen und Anwendungsprogrammierschnittstellen (APIs).						
2.3 Drahtlose Komponenten werden sicher konfiguriert und verwaltet.							
2.3.1	Für drahtlose Umgebungen, die mit der CDE verbunden sind oder Kontodaten übertragen, werden alle drahtlosen Anbieter-Standardeinstellungen bei der Installation geändert oder als sicher bestätigt, einschließlich, aber nicht beschränkt auf: • Standardmäßige drahtlose Verschlüsselungsschlüssel. • Passwörter auf drahtlosen Zugriffspunkten. • SNMP-Standardeinstellungen. • Alle anderen sicherheitsrelevanten drahtlosen Anbieter-Standardeinstellungen.	• Richtlinien und Prozeduren untersuchen. • Anbieterdokumentation überprüfen. • Drahtlose Konfigurationseinstellungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Dies beinhaltet, ist aber nicht beschränkt auf standardmäßige drahtlose Verschlüsselungsschlüssel, Passwörter für drahtlose Zugriffspunkte, SNMP-Standardeinstellungen und alle anderen sicherheitsrelevanten drahtlosen Anbieter-Standardeinstellungen.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
2.3.2	Für drahtlose Umgebungen, die mit der CDE verbunden sind oder Kontodaten übertragen, werden die drahtlosen Verschlüsselungsschlüssel wie folgt geändert:: • Immer dann, wenn Personal mit Kenntnis des Schlüssels das Unternehmen oder die Funktion verlassen, für die die Kenntnis notwendig war. • Immer dann, wenn vermutet wird oder bekannt ist, dass ein Schlüssel kompromittiert wurde.	• Schlüsselverwaltungsdokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐

Schutz von Kontodaten

Anforderung 3: Schutz von gespeicherten Kontodaten

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.1 Prozesse und Mechanismen zum Schutz gespeicherter Kontodaten sind definiert und verstanden.							
3.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 3 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
3.1.2	Die Rollen und Verantwortlichkeiten für die Durchführung der in Anforderung 3 genannten Tätigkeiten sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.2 Speicherung von Kontendaten wird auf einem Minimum gehalten.							
3.2.1	Die Speicherung von Kontodaten wird durch die Implementierung von Richtlinien, Verfahren und Prozessen zur Datenaufbewahrung und -entsorgung auf ein Minimum beschränkt, die mindestens Folgendes beinhalten: • Abdeckung für alle Speicherorte von gespeicherten Kontodaten. • Abdeckung aller sensiblen Authentifizierungsdaten (SAD), die vor Abschluss der Autorisierung gespeichert wurden. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Begrenzung der Datenspeichermenge und -aufbewahrungszeit auf das, was für gesetzliche oder behördliche und/oder Geschäfsanforderungen erforderlich ist. • Spezifische Aufbewahrungsanforderungen für gespeicherte Kontodaten, die die Länge der Aufbewahrungsfrist definieren und eine dokumentierte geschäftliche Begründung beinhalten. • Prozesse zum sicheren Löschen von Kontodaten oder wodurch Kontodaten nicht wiederhergestellt werden können, wenn sie gemäß der Aufbewahrungsrichtlinie nicht mehr benötigt werden. • Ein Prozess, um mindestens alle drei Monate zu verifizieren, ob gespeicherte Kontodaten, die die definierte Aufbewahrungsfrist überschreiten, sicher gelöscht oder nicht wiederhergestellt werden können. *(fortgesetzt)*	• Die Richtlinien, Prozeduren und Prozesse zur Aufbewahrung und Entsorgung von Daten untersuchen. • Personal befragen. • Dateien und Systemaufzeichnungen auf Systemkomponenten, in denen Kontodaten gespeichert sind, untersuchen. • Die Mechanismen beachten, die verwendet werden, um Kontodaten nicht wiederherstellbar zu machen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
	Hinweise zur Anwendbarkeit Wenn Kontodaten von einem TPSP gespeichert werden (zum Beispiel in einer Cloud-Umgebung), sind Entitäten dafür verantwortlich, mit ihren Dienstleistungsanbietern zusammenzuarbeiten, um zu verstehen, wie der TPSP diese Anforderung für die Entität erfüllt. Die Überlegungen beinhalten, sicherzustellen, dass alle geografischen Instanzen eines Datenelements sicher gelöscht werden. *Der obige Aufzählungspunkt (für die Abdeckung von SAD, die vor Abschluss der Autorisierung gespeichert wurden) ist eine bewährte Praktik bis zum 31. März 2025, danach ist er als Teil von Anforderung 3.2.1 erforderlich und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
3.3 Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert.							
3.3.1	SAD werden nach der Autorisierung nicht gespeichert, selbst wenn sie verschlüsselt sind. Alle empfangenen sensiblen Authentifizierungsdaten werden nach Abschluss des Autorisierungsprozesses nicht wiederherstellbar gemacht.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Systemkonfigurationen untersuchen. • Die sicheren Datenlöschprozesse beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Ein Teil dieses Hinweises zur Anwendbarkeit wurde für diesen SAQ absichtlich entfernt, da er nicht für Händlerbewertungen gilt.*. Sensible Authentifizierungsdaten beinhalten die in den Anforderungen 3.3.1.1 bis 3.3.1.3 genannten Daten.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.3.1.1	Der vollständige Inhalt einer Spur wird nach Abschluss des Autorisierungsprozesses nicht gespeichert.	• Datenquellen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Im normalen Geschäftsverlauf müssen möglicherweise folgende Datenelemente von der Spur aufbewahrt werden: • Name des Karteninhabers. • Primäre Kontonummer (PAN). • Ablaufdatum. • Dienstleistungscode. Um das Risiko zu minimieren, nur diese Datenelemente sicher speichern, die für den Geschäftsverkehr erforderlich sind.						
3.3.1.2	Der Kartenverifizierungscode wird nach Abschluss des Autorisierungsprozesses nicht gespeichert.	• Datenquellen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Der Kartenverifizierungscode ist die drei- oder vierstellige Zahl, die auf der Vorder- oder Rückseite einer Zahlungskarte aufgedruckt ist, die verwendet wird, um Transaktionen ohne Karte zu verifizieren.						
3.3.1.3	Die persönliche Identifikationsnummer (PIN) und die PIN-Sperre werden nach Abschluss des Autorisierungsprozesses nicht gespeichert.	• Datenquellen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit PIN-Sperren werden während des natürlichen Ablaufs von Transaktionsprozessen verschlüsselt, aber selbst wenn eine Entität die PIN-Sperre erneut verschlüsselt, darf er nach Abschluss des Autorisierungsprozesses nicht gespeichert werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.3.2	SAD, die elektronisch vor dem Abschluss der Autorisierung gespeichert werden, sind mit starker Kryptographie verschlüsselt.	• Datenspeicher und Systemkonfigurationen untersuchen. • Anbieterdokumentation untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Ob SAD vor der Autorisierung gespeichert werden dürfen, wird von den Organisationen bestimmt, die Einhaltungsprogramme verwalten (zum Beispiel Zahlungsmarken und Erwerber) verwalten. Erkundigen Sie sich bei diesen Organisationen nach zusätzlichen Kriterien. Diese Anforderung gilt für die gesamte Speicherung von SAD, auch wenn kein PAN in der Umgebung vorhanden ist. Siehe Anforderung 3.2.1 für eine zusätzliche Anforderung, die gilt, wenn SAD vor Abschluss der Autorisierung gespeichert wird. *Ein Teil dieses Hinweises zur Anwendbarkeit wurde für diesen SAQ absichtlich entfernt, da er nicht für Händlerbewertungen gilt.*. Diese Anforderung ersetzt weder die erforderliche Verwaltung von PIN-Sperren, noch bedeutet sie, dass eine ordnungsgemäß verschlüsselte PIN-Sperre erneut verschlüsselt werden muss. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
3.3.3	***Zusätzliche Anforderung für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen und sensible Authentifizierungsdaten speichern.***						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.4 Der Zugriff auf die Anzeigen des vollständigen PAN und die Möglichkeit zum Kopieren von PAN sind eingeschränkt.							
3.4.1	Die PAN wird bei der Anzeige maskiert (die BIN und die letzten vier Ziffern sind die maximale Anzahl anzuzeigender Ziffern), sodass nur Personal mit einem legitimen Geschäftsbedarf mehr als die BIN und die letzten vier Ziffern der PAN sehen kann.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Systemkonfigurationen untersuchen. • Die dokumentierte Liste der Rollen, die Zugriff auf mehr als die BIN und die letzten vier Ziffern der PAN benötigen (einschließlich der vollständigen PAN) untersuchen. • Anzeigen von PAN (z. B. auf dem Bildschirm, auf Papierquittungen) untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung ersetzt nicht die vorhandenen strengeren Anforderungen für Anzeigen von Karteninhaberdaten – zum Beispiel gesetzliche Anforderungen oder Anforderungen an Zahlungsmarken für Kassenbelege (POS). Diese Anforderung bezieht sich auf den Schutz von PAN, wenn sie auf Bildschirmen, Papierbelegen, Ausdrucken usw. angezeigt wird, und darf nicht mit Anforderung 3.5.1 zum Schutz von PAN bei der Speicherung, Verarbeitung oder Übertragung verwechselt werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.4.2	Bei der Verwendung von Fernzugriffs-Technologien verhindern technische Kontrollen das Kopieren und/oder Verlagern von PAN für das ganze Personal, mit Ausnahme von Personal mit dokumentierter, ausdrücklicher Autorisierung und einem legitimen, definierten Geschäftsbedarf.	• Dokumentierte Richtlinien und Prozeduren und dokumentierte Nachweise für technische Kontrollen untersuchen. • Konfigurationen für Fernzugriffstechnologien untersuchen. • Prozesse beachten. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Das Speichern oder Verlagern von PAN auf lokalen Festplatten, austauschbaren elektronischen Medien und anderen Speichergeräten bringt diese Geräte in den Geltungsbereich von PCI DSS. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.5 Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist.							
3.5.1	PAN wird überall dort, wo sie gespeichert wird, unlesbar gemacht, indem eine der folgenden Vorgehensweisen verwendet wird: • Einweg-Hashes basierend auf starker Kryptographie der gesamten PAN. • Abschneiden (Hashing kann nicht verwendet werden, um das abgeschnittene Segment von PAN zu ersetzen). – Wenn in einer Umgebung gehashte und abgeschnittene Versionen derselben PAN oder unterschiedliche Abschneidungsformate derselben PAN vorhanden sind, werden zusätzliche Kontrollen durchgeführt, damit die verschiedenen Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren • Verzeichnistoken. • Starke Kryptographie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren.	• Dokumentation über das System, das verwendet wird, um PAN unlesbar zu machen, untersuchen. • Datenrepositorien untersuchen. • Audit-Protokolle untersuchen, einschließlich Zahlungsanwendungsprotokolle. • Kontrollen untersuchen, um zu verifizieren, dass die gehashten und abgeschnittenen PANs nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt sowohl für PANs, die im primären Speicher (Datenbanken oder flachen Dateien wie Tabellenkalkulationen für Textdateien) gespeichert sind, als auch im nicht primären Speicher (Backup-, Audit-Protokolle, Ausnahme- oder Fehlerbehebungsprotokolle). Diese Anforderung schließt die Verwendung temporärer Dateien mit Klartext-PAN beim Ver- und Entschlüsseln von PAN nicht aus						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.5.1.1	Hashes, die verwendet werden, um PAN unlesbar zu machen (gemäß dem ersten Aufzählungspunkt von Anforderung 3.5.1) sind verschlüsselte kryptografische Hashes der gesamten PAN mit zugehörigen Schlüsselverwaltungsprozessen und -prozeduren gemäß den Anforderungen 3.6 und 3.7.	• Dokumentation über die verwendete Hash-Methode untersuchen. • Dokumentation über die Prozeduren und Prozesse der Schlüsselverwaltung untersuchen. • Datenrepositorien untersuchen. • Audit-Protokolle untersuchen, einschließlich Zahlungsanwendungsprotokolle.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Alle Anwendbarkeitshinweise für Anforderung 3.5.1 gelten auch für diese Anforderung. Prozesse und Verfahren zur Schlüsselverwaltung (Anforderungen 3.6 und 3.7) gelten nicht für Systemkomponenten, die zur Erzeugung einzelner verschlüsselter Hashes eines PAN zum Vergleich mit einem anderen System verwendet werden, wenn: • Die Systemkomponenten jeweils nur Zugriff auf einen Hash-Wert (Hash-Werte werden nicht auf dem System gespeichert) haben **UND** • Es keine anderen Kontodaten gibt, die auf demselben System wie die Hashes gespeichert sind. *Diese Anforderung wird bis zum 31. März 2025 als bewährte Praktik betrachtet, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden. Diese Anforderung wird den Aufzählungspunkt in Anforderung 3.5.1 für Einweg-Hashes ersetzen, sobald ihr wirksames Datum erreicht ist.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.5.1.2	Wenn eine Verschlüsselung auf Festplatten- oder Partitionsebene (anstatt einer Datenbankverschlüsselung auf Datei-, Spalten- oder Feldebene) verwendet wird, um PAN unlesbar zu machen, wird sie nur wie folgt implementiert: • Auf entfernbaren elektronischen Medien. **ODER** • Bei Verwendung für nicht entfernbare elektronische Medien wird PAN auch über einen anderen Mechanismus, der die Anforderung 3.5.1 erfüllt, unlesbar gemacht.	• Verschlüsselungsprozesse beachten. • Konfigurationen und/oder Anbieterdokumentation untersuchen. • Verschlüsselungsprozesse beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für jede Verschlüsselungsmethode, die automatisch Klartext-PAN bereitstellt, wenn ein System läuft, auch wenn ein autorisierter Benutzer diese Daten nicht ausdrücklich angefordert hat. Obwohl Festplatten- oder Partitionsverschlüsselung auf diesen Gerätetypen noch vorhanden sein kann, kann sie nicht der einzige Mechanismus sein, der verwendet wird, um auf diesen Systemen gespeicherte PANs zu schützen. Jede gespeicherte PAN muss außerdem gemäß Anforderung 3.5.1 unlesbar gemacht werden – zum Beispiel durch Abschneiden oder einen Verschlüsselungsmechanismus auf Datenebene. Die vollständige Festplattenverschlüsselung trägt zum Schutz der Daten bei einem physischen Verlust einer Festplatte bei und ist daher nur für entfernbare elektronische Medienspeichergeräte geeignet. Medien, die Teil einer Rechenzentrumsarchitektur sind (zum Beispiel Hot-Swap-fähige Laufwerke, Massensicherungen auf Band) gelten als nicht entfernbare elektronische Medien, für die Anforderung 3.5.1 gilt. Implementierungen der Festplatten- oder Partitionsverschlüsselung müssen auch alle anderen PCI DSS-Verschlüsselungs- und Schlüsselverwaltungsanforderungen erfüllen. *Ein Teil dieses Hinweises zur Anwendbarkeit wurde für diesen SAQ absichtlich entfernt, da er nicht für Händlerbewertungen gilt.* *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.5.1.3	Wenn eine Verschlüsselung auf Festplatten- oder Partitionsebene (anstatt einer Datenbankverschlüsselung auf Datei-, Spalten- oder Feldebene) verwendet wird, um PAN unlesbar zu machen, wird sie folgt verwaltet: • Der logische Zugriff wird separat und unabhängig von nativen Betriebssystem-Authentifizierungs- und Zugriffskontrollmechanismen verwaltet. • Entschlüsselungsschlüssel sind nicht mit Benutzerkonten assoziiert. • Authentifizierungsfaktoren (Passwörter, Passphrasen oder kryptografische Schlüssel), die den Zugriff auf nicht verschlüsselte Daten erlauben, werden sicher gespeichert.	• Systemkonfigurationen untersuchen. • Den Authentifizierungsprozess beachten. • Dateien, die Authentifizierungsfaktoren enthalten, untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Implementierungen der Festplatten- oder Partitionsverschlüsselung müssen auch alle anderen PCI DSS-Verschlüsselungs- und Schlüsselverwaltungsanforderungen erfüllen.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.6 Kryptografische Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, sind gesichert.							
3.6.1	Prozeduren werden definiert und implementiert, um kryptografische Schlüssel zu schützen, die verwendet werden, um gespeicherte Kontodaten vor Offenlegung und Missbrauch zu schützen, darunter: • Der Zugriff auf Schlüssel ist auf die erforderliche Anzahl von Verwahrern beschränkt. • Schlüsselverschlüsselungsschlüssel sind mindestens so stark wie die Datenverschlüsselungsschlüssel, die sie schützen. • Schlüsselverschlüsselungsschlüssel werden getrennt von Datenverschlüsselungsschlüsseln gespeichert. • Schlüssel werden an möglichst wenigen Orten und Formularen gespeichert.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für Schlüssel, die zum Schützen gespeicherter Kontodaten verwendet werden, und für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von datenverschlüsselnden Schlüsseln verwendet werden. Die Anforderung zum Schutz von Schlüsseln, die zum Schutz gespeicherter Kontodaten vor Offenlegung und Missbrauch verwendet werden, gilt sowohl für datenverschlüsselnde Schlüssel als auch für schlüsselverschlüsselnde Schlüssel. Da ein Schlüssel zum Verschlüsseln von Daten Zugriff auf viele Schlüssel zum Verschlüsseln von Daten gewähren kann, erfordern die Schlüssel zum Verschlüsseln von Schlüsseln starke Schutzmaßnahmen.						
3.6.1.1	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.6.1.2	Geheime und private Schlüssel, die zum Schützen gespeicherter Kontodaten verwendet werden, werden jederzeit in einem (oder mehreren) der folgenden Formate gespeichert: • Verschlüsselt mit einem Schlüssel zum Verschlüsseln, der mindestens so stark ist wie der Schlüssel zum Verschlüsseln von Daten, und der getrennt vom Schlüssel zum Verschlüsseln von Daten gespeichert wird. • Innerhalb eines sicheren kryptografischen Geräts (SCD), wie eines Hardware-Sicherheitsmoduls (HSM) oder eines PTS-zugelassenen Point-of-Interaction-Geräts. • Als mindestens zwei Schlüsselkomponenten voller Länge oder Schlüsselanteile, gemäß einer in der Branche anerkannten Methode.	• Dokumentierte Prozeduren untersuchen. • Systemkonfigurationen und Schlüsselspeicherstandorte untersuchen, einschließlich für Schlüsselverschlüsselungsschlüssel.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Es ist nicht erforderlich, dass öffentliche Schlüssel in einer dieser Formen gespeichert werden. Kryptografische Schlüssel, die als Teil eines Schlüsselverwaltungssystems (KMS) gespeichert werden, das SCDs verwendet, sind akzeptabel. Ein kryptografischer Schlüssel, der in zwei Teile geteilt ist, erfüllt diese Anforderung nicht. Als Schlüsselkomponenten oder Schlüsselanteile gespeicherte geheime oder private Schlüssel müssen über einen der Folgenden generiert werden: • Verwendung eines zugelassenen Zufallszahlengenerators und innerhalb einer SCD, **ODER** • Gemäß ISO 19592 oder einem gleichwertigen Industriestandard für die Generierung geheimer Schlüsselanteile.						
3.6.1.3	Zugriff auf kryptografische Schlüsselkomponenten im Klartext ist auf die geringste Anzahl von Verwahrern beschränkt.	• Benutzerzugriffslisten untersuchen.	☐	☐	☐	☐	☐
3.6.1.4	Kryptografische Schlüssel werden an möglichst wenigen Orten gespeichert.	• Schlüsselspeicherstandorte beachten. • Prozesse beachten.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.7 Wenn Kryptographie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüsselverwaltungsprozesse und -prozeduren definiert und implementiert, die alle Aspekte des Schlüssellebenszyklus abdecken.							
3.7.1	Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um die Generierung von starken sicheren kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten einzuschließen.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Die Methode zum Erzeugen von Schlüsseln beachten.	☐	☐	☐	☐	☐
3.7.2	Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um sichere Verteilung von kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten einzuschließen.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Die Methode zum Verteilen von Schlüsseln beachten.	☐	☐	☐	☐	☐
3.7.3	Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um sichere Speicherung von kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten einzuschließen.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Die Methode zum Speichern von Schlüsseln beachten.	☐	☐	☐	☐	☐
3.7.4	Richtlinien und Verfahren zur Schlüsselverwaltung werden für kryptografische Schlüsseländerungen für Schlüssel implementiert, die das Ende ihrer Verschlüsselungszeitdauer erreicht haben, wie vom jeweiligen Anwendungsanbieter oder Schlüsselbesitzer definiert ist und auf den bewährten Praktiken und Richtlinien der Branche basiert, einschließlich der folgenden: • Eine definierte Kryptozeitdauer für jeden verwendeten Schlüsseltyp. • Einen Prozess für Schlüsseländerungen am Ende der definierten Kryptozeitdauer.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Personal befragen. • Schlüsselspeicherstandorte beachten.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.7.5	Prozeduren zur Schlüsselverwaltung werden implementiert, um die Aussonderung, den Ersatz oder die Zerstörung von Schlüsseln, die zum Schutz gespeicherter Kontodaten verwendet werden, nach Bedarf zu umfassen, wenn: • Der Schlüssel das Ende seiner definierten Kryptozeitdauer erreicht hat. • Die Integrität des Schlüssels geschwächt wurde, auch wenn Personal mit Kenntnis einer Klartext-Schlüsselkomponente das Unternehmen verlässt oder die Rolle, für die die Schlüsselkomponente bekannt war, verlässt. • Wenn vermutet wird oder bekannt ist, dass der Schlüssel kompromittiert wurde. Ausgesonderte oder ersetzte Schlüssel werden nicht für Verschlüsselungsbetriebe verwendet.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Wenn ausgesonderte oder ersetzte kryptografische Schlüssel aufbewahrt werden müssen, müssen diese Schlüssel sicher archiviert werden (zum Beispiel mithilfe eines Schlüsselverschlüsselungsschlüssels).						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
3.7.6	Wenn manuelle Betriebe zur Verwaltung von kryptografischen Klartextschlüsseln von Personal durchgeführt werden, werden Richtlinien und Prozeduren zur Schlüsselverwaltung implementiert, einschließlich die Verwaltung dieser Betriebe unter Verwendung von geteiltem Wissen und doppelter Kontrolle.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Personal befragen. • Prozesse beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Kontrolle gilt für manuelle Schlüsselverwaltungsbetriebe. Ein kryptografischer Schlüssel, der einfach in zwei Teile geteilt ist, erfüllt diese Anforderung nicht. Als Schlüsselkomponenten oder Schlüsselanteile gespeicherte geheime oder private Schlüssel müssen über einen der Folgenden generiert werden: • Verwendung eines zugelassenen Zufallszahlengenerators und in einem sicheren kryptografischen Gerät (SCD), wie einem Hardware-Sicherheitsmodul (HSM) oder einem PTS-zugelassenen Ort der Interaktion-Gerät, **ODER** • Gemäß ISO 19592 oder einem gleichwertigen Industriestandard für die Generierung geheimer Schlüsselanteile.						
3.7.7	Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um die Verhinderung eines nicht autorisierten Austauschs kryptographischer Schlüssel einzuschließen.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Personal befragen. • Prozesse beachten.	☐	☐	☐	☐	☐
3.7.8	Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um zu enthalten, dass die Verwahrer von kryptografischen Schlüsseln formell bestätigen (schriftlich oder elektronisch), dass sie ihre Verantwortlichkeiten als Schlüsselverwahrer verstehen und akzeptieren.	• Dokumentierte Schlüsselverwaltungs-Richtlinien und Prozeduren untersuchen. • Dokumentation oder andere Nachweise für die Bestätigung der Schlüsselverwalter überprüfen.	☐	☐	☐	☐	☐
3.7.9	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter*						

Anforderung 4: Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
4.1 Prozesse und Mechanismen zum Schutz von Karteninhaberdaten mit starker Kryptographie bei der Übertragung über offene, öffentliche Netze werden definiert und verstanden.							
4.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 4 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
4.1.2	Die Rollen und Verantwortlichkeiten für die Durchführung der in Anforderung 4 genannten Tätigkeiten sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
4.2 PAN wird während der Übertragung mit starker Kryptographie geschützt.							
4.2.1	Starke Kryptografie- und Sicherheitsprotokolle werden implementiert, um PAN während der Übertragung wie folgt über offene, öffentliche Netzwerke zu schützen:						
	• Es werden nur vertrauenswürdige Schlüssel und Zertifikate akzeptiert.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Personal befragen. • Systemkonfigurationen untersuchen. • Übertragungen von Karteninhaberdaten untersuchen. • Schlüssel und Zertifikate untersuchen.	☐	☐	☐	☐	☐
	• Zertifikate, die zum Schutz von PAN bei der Übertragung über offene, öffentliche Netze verwendet werden, werden als gültig bestätigt und sind nicht abgelaufen oder widerrufen. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.*		☐	☐	☐	☐	☐
	• Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen und unterstützt keinen Rückfall auf oder die Verwendung von unsicheren Versionen, Algorithmen, Schlüsselgrößen oder Implementierungen.		☐	☐	☐	☐	☐
	• Die Verschlüsselungsstärke ist für die verwendete Verschlüsselungsmethodik angemessen.		☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Ein selbstsigniertes Zertifikat kann auch akzeptabel sein, wenn das Zertifikat von einer internen CA innerhalb der Organisation ausgestellt wird, der Autor des Zertifikats bestätigt und das Zertifikat verifiziert ist – zum Beispiel per Hash oder Unterschrift – und nicht abgelaufen ist. *Der obige Aufzählungspunkt (zur Bestätigung, dass Zertifikate, die zum Schutz von PAN während der Übertragung über offene, öffentliche Netzwerke verwendet werden, gültig sind und nicht abgelaufen oder widerrufen sind) ist eine bewährte Praktik bis zum 31. März 2025, danach wird er als Teil von Anforderung 4.2.1 benötigt und muss bei einer PCI-DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
4.2.1.1	Es wird ein Inventar der vertrauenswürdigen Schlüssel und Zertifikate der Entität geführt, die zum Schutz von PAN während der Übertragung verwendet werden.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Das Inventar von vertrauenswürdigen Schlüsseln und Zertifikaten untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
4.2.1.2	Drahtlose Netzwerke, die PAN übertragen oder mit der CDE verbunden sind, verwenden bewährte Praktiken der Branche, um eine starke Kryptographie für die Authentifizierung und Übertragung zu implementieren.	• Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐
4.2.2	PAN wird immer mit starker Kryptographie gesichert, wenn es über Messaging-Technologien für Endbenutzer gesendet wird.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Systemkonfigurationen und Anbieterdokumentation untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt auch, wenn ein Kunde oder ein anderer Dritter die Zusendung von PAN über Endbenutzer-Messaging-Technologien anfordert. Es kann vorkommen, dass eine Entität unaufgeforderte Karteninhaberdaten über einen unsicheren Kommunikationskanal erhält, der nicht für Übertragungen sensibler Daten vorgesehen ist. In dieser Situation kann die Entität entweder den Kanal in den Geltungsbereich ihrer CDE aufnehmen und ihn gemäß PCI DSS sichern oder die Karteninhaberdaten löschen und Maßnahmen implementieren, um zu verhindern, dass der Kanal für Karteninhaberdaten verwendet wird.						

Wartung eines Programms zur Verwaltung von Schwachstellen

Anforderung 5: Schutz aller Systeme und Netzwerke vor bösartiger Software

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
5.1 Prozesse und Mechanismen zum Schutz aller Systeme und Netzwerke vor böswilliger Software sind definiert und verstanden.							
5.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 5 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
5.1.2	Die Rollen und Zuständigkeiten für die Durchführung der Aktivitäten gemäß Anforderung 5 sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
5.2 Böswillige Software (Malware) wird verhindert oder erfasst und beseitigt.							
5.2.1	Eine Anti-Malware Lösung(en) werden auf allen Systemkomponenten bereitgestellt, mit Ausnahme der Systemkomponenten, die in regelmäßigen Bewertungen gemäß Anforderung 5.2.3 identifiziert wurden, die zu dem Schluss kommen, dass die Systemkomponenten nicht durch Malware gefährdet sind.	• Systemkomponenten untersuchen. • Die regelmäßigen Auswertungen untersuchen.	☐	☐	☐	☐	☐
5.2.2	Die eingesetzte(n) Anti-Malware-Lösung(en): • Erkennt alle bekannten Arten von Malware. • Entfernt, sperrt oder dämmt alle bekannten Arten von Malware ein.	• Anbieterdokumentation untersuchen. • Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
5.2.3	Alle Systemkomponenten, die nicht durch Malware gefährdet sind, werden regelmäßig bewertet, um Folgendes zu beinhalten: • Eine dokumentierte Liste aller Systemkomponenten, die nicht durch Malware gefährdet sind. • Identifizierung und Bewertung von sich entwickelnden Malware-Bedrohungen für diese Systemkomponenten. • Bestätigung, ob solche Systemkomponenten weiterhin keinen Anti-Malware-Schutz benötigen.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Personal befragen. • Die Liste der Systemkomponenten, bei denen kein Malware-Risiko besteht, untersuchen und sie mit den Systemkomponenten ohne eingesetzte Anti-Malware-Lösung vergleichen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Von dieser Anforderung abgedeckte Systemkomponenten sind diejenigen, für die keine Anti-Malware-Lösung gemäß Anforderung 5.2.1 eingesetzt wurde.						
5.2.3.1	Die Häufigkeit der regelmäßigen Bewertungen von Systemkomponenten, die als nicht gefährdet für Malware identifiziert wurden, wird in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	• Die gezielte Risikoanalyse untersuchen. • Dokumentierte Ergebnisse von regelmäßigen Auswertungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
5.3 Anti-Malware-Mechanismen und Prozesse sind aktiv, werden gewartet und überwacht.							
5.3.1	Die Anti-Malware-Lösung(en) wird (werden) durch automatische Aktualisierungen auf dem neuesten Stand gehalten.	• Anti-Malware-Lösungs-Konfigurationen untersuchen, einschließlich aller Master-Installationen. • Systemkomponenten und Protokolle untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
5.3.2	Die Anti-Malware-Lösung(en): • Führt regelmäßige Scans und aktive oder Echtzeit-Scans durch **ODER** • Führt eine kontinuierliche Verhaltensanalyse von Systemen oder Prozessen durch.	• Anti-Malware-Lösungs-Konfigurationen untersuchen, einschließlich aller Master-Installationen. • Systemkomponenten untersuchen. • Protokolle und Scan-Ergebnisse untersuchen.	☐	☐	☐	☐	☐
5.3.2.1	Wenn regelmäßige Malware-Scans durchgeführt werden, um Anforderung 5.3.2 zu erfüllen, wird die Häufigkeit der Scans in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	• Die gezielte Risikoanalyse untersuchen. • Dokumentierte Ergebnisse von regelmäßigen Malware-Scans untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für Entitäten, die regelmäßige Malware-Scans durchführen, um Anforderung 5.3.2 zu erfüllen. Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
5.3.3	Für entfernbare elektronische Medien führt die Anti-Malware-Lösung: • automatische Scans durch, wenn die Medien eingelegt, verbunden oder logisch angebracht werden, **ODER** • eine kontinuierliche Verhaltensanalyse von Systemen oder Prozessen durch, wenn die Medien eingelegt, verbunden oder logisch angebracht werden.	• Konfigurationen der Anti-Malware-Lösung(en) untersuchen. • Systemkomponenten mit entfernbaren elektronischen Medien untersuchen. • Protokolle und Scan-Ergebnisse untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
5.3.4	Audit-Protokolle für die Anti-Malware-Lösung(en) werden gemäß Anforderung 10.5.1 aktiviert und aufbewahrt.	• Konfigurationen der Anti-Malware-Lösung(en) untersuchen.	☐	☐	☐	☐	☐
5.3.5	Anti-Malware-Mechanismen können von Benutzern nicht deaktiviert oder geändert werden, es sei denn, dies wird von der Geschäftsleitung im Einzelfall für eine begrenzten Zeitdauer ausdrücklich dokumentiert und genehmigt.	• Anti-Malware-Konfigurationen untersuchen. • Prozesse beachten. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Anti-Malware-Lösungen dürfen nur dann vorübergehend deaktiviert werden, wenn ein berechtigter technischer Bedarf besteht, der von der Verwaltung im Einzelfall genehmigt wird. Wenn der Anti-Malware-Schutz für einen bestimmten Zweck deaktiviert werden muss, muss dieses formell autorisiert werden. Für die Zeitdauer, in dem der Anti-Malware-Schutz nicht aktiv ist, müssen möglicherweise zusätzliche Sicherheitsmaßnahmen implementiert werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
5.4 Anti-Phishing-Mechanismen schützen Benutzer vor Phishing-Angriffen.							
5.4.1	Prozesse und automatisierte Mechanismen sind vorhanden, um Phishing-Angriffe zu erkennen und das Personal davor zu schützen.	• Implementierte Prozesse beachten. • Mechanismen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Der Schwerpunkt dieser Anforderung liegt auf dem Schutz des Personals mit Zugriff auf Systemkomponenten im Geltungsbereich von PCI DSS. Die Erfüllung dieser Anforderung an technische und automatisierte Kontrollen zur Erkennung und zum Schutz des Personals vor Phishing ist nicht dasselbe wie Anforderung 12.6.3.1 für Schulung zum Sicherheitsbewusstsein. Die Erfüllung dieser Anforderung erfüllt auch nicht die Anforderung, das Personal mit Sicherheitsbewusstsein zu schulen und umgekehrt. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Software

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.1 Prozesse und Mechanismen zur Entwicklung und Wartung von sicheren Systemen und Software werden definiert und verstanden.							
6.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 6 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
6.1.2	Die Rollen und Zuständigkeiten für die Durchführung der Aktivitäten gemäß Anforderung 6 sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
6.2 Maßgeschneiderte und kundenspezifische Software werden sicher entwickelt.							
6.2.1	Maßgeschneiderte und kundenspezifische Software werden sicher wie folgt entwickelt: • Basierend auf Industriestandards und/oder bewährten Praktiken für eine sichere Entwicklung. • Gemäß PCI DSS (zum Beispiel sichere Authentifizierung und Protokollierung). • Einbeziehung von Berücksichtigung von Fragen der Informationssicherheit in jeder Phase des Softwareentwicklungs-Lebenszyklus.	• Dokumentierte Softwareentwicklungsverfahren untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Dies gilt für alle Software, die für oder von der Entität für den eigenen Gebrauch entwickelt wurde. Dies beinhaltet sowohl maßgeschneiderte als auch kundenspezifische Software. Dies gilt nicht für Software von Drittanbietern.						

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.2.2	Softwareentwicklungspersonal, das an maßgeschneiderter und kundenspezifischer Software arbeitet, wird mindestens einmal alle 12 Monate wie folgt geschult: • über Softwaresicherheit, die für ihre Tätigkeitsfunktion und Entwicklungssprachen relevant ist. • Einschließlich sicheres Softwaredesign und sichere Codierungstechniken. • Einschließlich, wenn Sicherheitstesttools verwendet werden, wie die Tools zum Erkennen von Schwachstellen in Software verwendet werden.	• Dokumentierte Softwareentwicklungsverfahren untersuchen. • Schulungsaufzeichnungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Das Softwareentwicklungspersonal bleibt über sichere Entwicklungspraktiken informiert; Softwaresicherheit; und Angriffe gegen die Sprachen, Rahmenwerke oder Anwendungen, die sie entwickeln. Das Personal kann bei Bedarf auf Hilfe und Anleitungen zugreifen.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.2.3	Maßgeschneiderte und kundenspezifische Software wird vor der Freigabe für die Produktion oder für Kunden überprüft, um potenzielle Codierungsschwachstellen wie folgt zu identifizieren und zu korrigieren: • Code-Überprüfungen stellen sicher, dass Code gemäß den Richtlinien für sichere Codierung entwickelt wird. • Code-Überprüfungen suchen sowohl nach bestehenden als auch nach neuen Software-Schwachstellen. • Entsprechende Korrekturen werden vor der Freigabe implementiert.	• Dokumentierte Softwareentwicklungsverfahren untersuchen. • Verantwortliches Personal befragen. • Nachweise für Änderungen an maßgeschneiderter und kundenspezifischer Software untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung für Code-Überprüfungen gilt für alle maßgeschneiderte und kundenspezifische Software (sowohl intern als auch öffentlich zugänglich) als Teil des Systementwicklungslebenszyklus. Öffentlich zugängliche Webanwendungen unterliegen ebenfalls zusätzlichen Kontrollen, um laufende Bedrohungen und Schwachstellen nach der Implementierung zu adressieren, wie in der PCI-DSS-Anforderung 6.4 definiert. Code-Überprüfungen können entweder mit manuellen oder automatisierten Prozessen oder einer Kombination aus beiden durchgeführt werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.2.3.1	Wenn für maßgeschneiderte und benutzerdefinierte Software vor der Freigabe für die Produktion manuelle Code-Überprüfungen durchgeführt werden, dann werden Codeänderungen: • Von anderen Personen als dem ursprünglichen Code-Autor überprüft, und die sich mit Code-Überprüfungs-Techniken und sicheren Codierungspraktiken auskennen. • Vor der Freigabe von der Geschäftsleitung geprüft und genehmigt.	• Dokumentierte Softwareentwicklungsverfahren untersuchen. • Verantwortliches Personal befragen. • Nachweise für Änderungen an maßgeschneiderter und kundenspezifischer Software untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Manuelle Code-Überprüfungen können durch sachkundiges internes Personal oder sachkundiges Personal Dritter durchgeführt werden. Eine Person, der formell die Verantwortung für die Freigabekontrolle übertragen wurde und die weder der ursprüngliche Code-Autor noch der Code-Überprüfer ist, erfüllt die Kriterien der Verwaltung.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.2.4	Softwareentwicklungstechniken oder andere Methoden werden von Softwareentwicklungspersonal für maßgeschneiderte und kundenspezifische Software definiert und verwendet, um übliche Softwareangriffe und damit verbundene Schwachstellen in maßgeschneiderter und kundenspezifischer Software zu verhindern oder abzuschwächen, einschließlich, aber nicht beschränkt auf Folgendes:						
	• Injektionsangriffe, einschließlich SQL-, LDAP-, XPath- oder andere Befehls-, Parameter-, Objekt-, Fehler- oder injektionsartige Mängel.	• Dokumentierte Prozeduren untersuchen. • Verantwortliches Softwareentwicklungspersonal befragen.	☐	☐	☐	☐	☐
	• Angriffe auf Daten und Datenstrukturen, einschließlich Versuche, Puffer, Zeiger, Eingabedaten oder gemeinsam genutzte Daten zu manipulieren.		☐	☐	☐	☐	☐
	• Angriffe auf die Kryptografienutzung, einschließlich Versuche, schwache, unsichere oder unangemessene kryptografische Implementierungen, Algorithmen, Verschlüsselungssammlungen oder Betriebsmodi auszunutzen.		☐	☐	☐	☐	☐
	• Angriffe auf die Geschäftslogik, einschließlich Versuche, Anwendungsmerkmale und -funktionen durch die Manipulation von APIs, Kommunikationsprotokollen und -kanälen, kundenseitigen Funktionen oder anderen System-/Anwendungsfunktionen und -ressourcen zu missbrauchen oder zu umgehen. Dazu gehören Cross-Site-Scripting (XSS) und Cross-Site-Request-Forgery (CSRF). *(fortgesetzt)*		☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
	• Angriffe auf Zugriffskontrollmechanismen, einschließlich Versuche, Identifizierungs-, Authentifizierungs-, oder Autorisierungsmechanismen zu umgehen oder zu missbrauchen, oder Versuche, Schwachstellen bei der Implementierung solcher Mechanismen auszunutzen.		☐	☐	☐	☐	☐
	• Angriffe über alle „Hochrisiko“-Schwachstellen, die im Schwachstellenidentifizierungsprozess identifiziert wurden, wie in Anforderung 6.3.1 definiert.		☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Dies gilt für alle Software, die für oder von der Entität für den eigenen Gebrauch entwickelt wurde. Dies beinhaltet sowohl maßgeschneiderte als auch kundenspezifische Software. Dies gilt nicht für Software von Drittanbietern.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.3 Sicherheitsschwachstellen werden identifiziert und adressiert.							
6.3.1	Sicherheitsschwachstellen werden identifiziert und wie folgt verwaltet: • Neue Sicherheitsschwachstellen werden mithilfe von branchenweit anerkannten Quellen für Sicherheitsschwachstelleninformationen identifiziert, einschließlich Warnungen von internationalen und nationalen Computer-Notfallteams (CERTs). • Schwachstellen werden basierend auf den bewährten Praktiken der Branche und der Berücksichtigung potenzieller Auswirkungen einer Risikoeinstufung zugewiesen. • Risikoeinstufungen identifizieren mindestens alle Schwachstellen, die als hochriskant oder kritisch für die Umgebung angesehen werden. • Schwachstellen für maßgeschneiderte und kundenspezifische Software von Drittanbietern (zum Beispiel Betriebssysteme und Datenbanken) werden abgedeckt.	• Richtlinien und Prozeduren untersuchen. • Verantwortliches Personal befragen. • Dokumentation untersuchen. • Prozesse beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung wird nicht durch die Durchführung von Schwachstellen-Scans gemäß den Anforderungen 11.3.1 und 11.3.2 erfüllt, sondern ist zusätzlich dazu erforderlich. Diese Anforderung gilt für einen Prozess zur aktiven Überwachung von Branchenquellen auf Schwachstelleninformationen und für die Entität, um die mit jeder Schwachstelle verbundene Risikoeinstufung zu bestimmen.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.3.2	Ein Inventar von maßgeschneiderter und kundenspezifischer Software und Softwarekomponenten von Dritten, die in maßgeschneiderte und kundenspezifische Software integriert sind, wird gepflegt, um das Schwachstellen- und die Patch-Verwaltung zu erleichtern.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
6.3.3	Alle Systemkomponenten werden vor bekannten Schwachstellen geschützt, indem anwendbare Sicherheitspatches/Aktualisierungen wie folgt installiert werden: • Patches/Aktualisierungen für kritische Schwachstellen werden gemäß dem Risikoeinstufungsprozess in Anforderung 6.3.1 identifiziert, werden innerhalb eines Monats der Veröffentlichung installiert. • Alle anderen anwendbaren Sicherheitspatches/Aktualisierungen werden innerhalb eines angemessenen Zeitrahmens installiert, der von der Entität vorgenommenen Bewertung der Kritikalität des Risikos für die Umwelt, die gemäß der Risikoeinstufung in Anforderung 6.3.1 bestimmt wurde.	• Richtlinien und Prozeduren untersuchen. • Systemkomponenten und verwandte Software untersuchen. • Vergleichen der Liste der installierten Sicherheits-Patches mit den aktuellen Anbieter-Patch-Listen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.4 Öffentlich zugängliche Webanwendungen sind gegen Angriffe geschützt.							
6.4.1	Für öffentlich zugängliche Webanwendungen werden laufend neue Bedrohungen und Schwachstellen adressiert und diese Anwendungen werden wie folgt vor bekannten Angriffen geschützt: • Überprüfung öffentlich zugänglicher Webanwendungen mit manuellen oder automatisierten Tools oder Methoden zur Sicherheitsbewertung von Anwendungsschwachstellen wie folgt: – Mindestens einmal alle 12 Monate und nach bedeutenden Änderungen. – Von einer Entität, die auf Anwendungssicherheit spezialisiert ist. – Einschließlich mindestens aller gängigen Softwareangriffe in Anforderung 6.2.4. – Alle Schwachstellen werden gemäß Anforderung 6.3.1 eingestuft. – Alle Schwachstellen werden korrigiert. – Die Anwendung wird nach den Korrekturen erneut evaluiert **ODER** • Eine automatisierte technische Lösung(en) wird installiert, die webbasierte Angriffe wie folgt kontinuierlich erkennt und verhindert: – Wird vor öffentlich zugänglichen Webanwendungen installiert, um webbasierte Angriffe zu erkennen und zu verhindern. – Aktiv laufend und gegebenenfalls auf dem neuesten Stand. – Generieren von Audit-Protokollen. *(fortgesetzt)*	• Dokumentierte Prozesse untersuchen. • Personal befragen. • Aufzeichnungen der Anwendungssicherheitsbewertungen untersuchen. • Systemkonfigurationseinstellungen und Audit-Protokolle untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
	– Konfiguriert, um entweder webbasierte Angriffe zu blockieren oder eine Warnung zu generieren, die sofort untersucht wird.						
	Hinweise zur Anwendbarkeit Diese Bewertung ist nicht dasselbe wie die für Anforderung 11.3.1 und 11.3.2 durchgeführten Schwachstellen-Scans. Diese Anforderung wird durch Anforderung 6.4.2 nach dem 31. März 2025 ersetzt, wenn Anforderung 6.4.2 in Kraft tritt.						
6.4.2	Für öffentlich zugängliche Webanwendungen wird eine automatisierte technische Lösung eingesetzt, die webbasierte Angriffe kontinuierlich erkennt und verhindert, mit mindestens den folgenden: • Wird vor öffentlich zugänglichen Webanwendungen installiert, und ist konfiguriert, um webbasierte Angriffe zu erkennen und zu verhindern. • Aktiv laufend und gegebenenfalls auf dem neuesten Stand. • Generieren von Audit-Protokollen. • Konfiguriert, um entweder webbasierte Angriffe zu blockieren oder eine Warnung zu generieren, die sofort untersucht wird.	• Die Systemkonfigurationseinstellungen untersuchen. • Audit-Protokolle untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese neue Anforderung wird Anforderung 6.4.1 ersetzen, sobald ihr effektives Datum erreicht ist. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.4.3	Alle Zahlungsseitenskripte, die im Browser des Verbrauchers geladen und ausgeführt werden, werden wie folgt verwaltet:						
	• Es wird eine Methode implementiert, um zu bestätigen, dass jedes Skript autorisiert ist.	• Richtlinien und Prozeduren untersuchen. • Verantwortliches Personal befragen. • Inventaraufzeichnungen untersuchen. • Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐
	• Es wird eine Methode implementiert, um die Integrität jedes Skripts sicherzustellen.		☐	☐	☐	☐	☐
	• Es wird ein Inventar aller Skripte mit schriftlicher geschäftlicher oder technischer Begründung geführt, warum jedes benötigt wird.		☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Diese Anforderung gilt für alle Skripte, die aus der Umgebung der Entität geladen werden und für Skripte, die von Dritten und Vierten geladen werden. Diese Anforderung gilt auch für Skripte auf der/den Webseite(n) des Unternehmens, die eine eingebettete Zahlungsseite/ein eingebettetes Zahlungsformular eines TPSP/Zahlungsabwicklers enthalten (z. B. ein oder mehrere Inline-Frames oder iframes). Diese Anforderung gilt nicht für ein Unternehmen für Skripte in einer eingebetteten Zahlungsseite/einem eingebetteten Zahlungsformular eines TPSP/Zahlungsabwicklers (z. B. ein oder mehrere Iframes), wenn das Unternehmen eine Zahlungsseite/ein Zahlungsformular eines TPSP/Zahlungsabwicklers auf seiner Webseite enthält. Für die Verwaltung der Skripte in der eingebetteten Zahlungsseite/dem eingebetteten Zahlungsformular des TPSP/Zahlungsabwicklers ist der TPSP/Zahlungsabwickler in Übereinstimmung mit dieser Anforderung verantwortlich. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.5 Änderungen an allen Systemkomponenten werden sicher verwaltet.							
6.5.1	Änderungen an allen Systemkomponenten in der Produktionsumgebung werden gemäß etablierter Prozeduren vorgenommen, die Folgende beinhalten: • Grund für und Beschreibung der Änderung. • Dokumentation der Auswirkung auf die Sicherheit. • Dokumentierte Änderungsgenehmigung durch autorisierte Parteien. • Testen um zu verifizieren, dass die Änderung die Systemsicherheit nicht beeinträchtigt. • Für maßgeschneiderte und kundenspezifische Softwareänderungen werden alle Aktualisierungen auf Einhaltung von Anforderung 6.2.4 getestet, bevor sie in der Produktion eingesetzt werden. • Prozeduren, um Versagen zu adressieren und in einen sicheren Zustand zuückzukehren.	• Dokumentierte Änderungskontrollprozeduren untersuchen. • Kürzliche Änderungen an Systemkomponenten untersuchen und Änderungen zu der Änderungskontrolldokumentation verfolgen. • Änderungskontrolldokumentation untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.5.2	Nach Abschluss einer bedeutenden Änderung wird bestätigt, dass alle anwendbaren PCI DSS-Anforderungen auf allen neuen oder geänderten Systemen und Netzwerken vorhanden sind, und die Dokumentation wird gegebenenfalls aktualisiert.	• Dokumentation auf wesentliche Änderungen untersuchen. • Personal befragen. • Die betroffenen Systeme/Netzwerke beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese bedeutenden Änderungen sollten auch erfasst und in der jährlichen PCI DSS-Geltungsbereichs-Bestätigungsaktivität der Entität gemäß Anforderung 12.5.2 widergespiegelt werden.						
6.5.3	Vorproduktionsumgebungen werden von Produktionsumgebungen getrennt und die Trennung wird mit Zugriffskontrollen erzwungen.	• Richtlinien und Prozeduren untersuchen. • Netzwerkdokumentation und Konfigurationen von Netzwerksicherheitskontrollen untersuchen. • Zugriffskontrolleinstellungen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
6.5.4	Rollen und Funktionen sind zwischen Produktions- und Vorproduktionsumgebungen getrennt, um Rechenschaftspflicht bereitzustellen, sodass nur überprüfte und genehmigte Änderungen eingesetzt werden.	• Richtlinien und Prozeduren untersuchen. • Prozesse beachten. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit In Umgebungen mit begrenztem Personal, in denen Personen mehrere Rollen oder Funktionen durchführen, kann dasselbe Ziel mit zusätzlichen prozeduralen Kontrollen erreicht werden, die Rechenschaftspflicht bereitstellen. Zum Beispiel kann ein Entwickler auch ein Administrator sein, der ein Konto auf Administratorebene mit erhöhten Privilegien in der Entwicklungsumgebung verwendet und für seine Entwicklerrolle ein separates Konto mit Zugriff auf Benutzerebene auf die Produktionsumgebung verwendet.						
6.5.5	Live-PANs werden nicht in Vorproduktionsumgebungen verwendet, es sei denn, diese Umgebungen sind in der CDE enthalten und gemäß allen anwendbaren PCI DSS-Anforderungen geschützt.	• Richtlinien und Prozeduren untersuchen. • Testprozesse beachten. • Personal befragen. • Testdaten aus der Vorproduktion untersuchen.	☐	☐	☐	☐	☐
6.5.6	Testdaten und Testkonten werden von Systemkomponenten entfernt, bevor das System in Produktion geht.	• Richtlinien und Prozeduren untersuchen. • Testprozesse für Standardsoftware und für Inhouse-Anwendungen beachten. • Personal befragen. • Daten und Konten für kürzlich installierte oder aktualisierte handelsübliche Software und interne Anwendungen untersuchen.	☐	☐	☐	☐	☐

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach geschäftlichem Bedarf

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
7.1 Prozesse und Mechanismen zur Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten durch geschäftlichen Bedarf werden definiert und verstanden.							
7.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 7 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
7.1.2	Die Rollen und Verantwortlichkeiten für die Durchführung der in Anforderung 7 genannten Tätigkeiten sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
7.2 Der Zugriff auf Systemkomponenten und Daten wird entsprechend definiert und zugewiesen.							
7.2.1	Ein Zugriffskontrollmodell wird definiert und umfasst die Zugriffsgewährung wie folgt: • Angemessener Zugriff abhängig von den Geschäfts- und Zugriffsanforderungen der Entität. • Zugriff auf Systemkomponenten und Datenressourcen, die auf der Jobklassifizierung und den Funktionen der Benutzer basieren. • Die geringsten erforderlichen Privilegien (zum Beispiel Benutzer, Administrator), um eine Jobfunktion durchzuführen.	• Dokumentierte Richtlinien und Prozeduren untersuchen. • Personal befragen. • Zugriffskontrollmodelleinstellungen untersuchen.	☐	☐	☐	☐	☐
7.2.2	Der Zugriff wird Benutzern, einschließlich privilegierten Benutzern, basierend auf Folgendem zugewiesen: • Jobklassifizierung und Funktion. • Geringste Privilegien, die zur Erfüllung der beruflichen Aufgaben erforderlich sind.	• Richtlinien und Prozeduren untersuchen. • Benutzerzugriffseinstellungen, einschließlich für privilegierte Benutzer untersuchen. • Verantwortliches Verwaltungspersonal befragen. • Personal, das für die Zuweisung des Zugriffs verantwortlich ist befragen.	☐	☐	☐	☐	☐
7.2.3	Erforderliche Privilegien werden von autorisiertem Personal genehmigt.	• Richtlinien und Prozeduren untersuchen. • Benutzer-IDs und zugewiesene Privilegien untersuchen. • Dokumentierte Genehmigungen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
7.2.4	Alle Benutzerkonten und zugehörigen Zugriffsrechte, einschließlich Konten von Dritten/Anbietern, werden wie folgt überprüft: • Mindestens einmal alle sechs Monate. • Um sicherzustellen, dass Benutzerkonten und Zugriff je nach Jobfunktion angemessen bleiben. • Jeder unangemessene Zugriff wird adressiert. • Die Verwaltung bestätigt, dass der Zugriff weiterhin angemessen ist.	• Richtlinien und Prozeduren untersuchen. • Verantwortliches Personal befragen. • Dokumentierte Ergebnisse von regelmäßigen Überprüfungen von Benutzerkonten untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Benutzerkonten und verwandte Zugriffsprivilegien, einschließlich derjenigen, die von Mitarbeitern und Dritten/Anbietern verwendet werden, und für Konten, die für den Zugriff auf Cloud-Dienstleistungen von Dritten verwendet werden. Siehe Anforderungen 7.2.5 und 7.2.5.1 und 8.6.1 bis 8.6.3 für Kontrollen für Anwendungs- und Systemkonten. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
7.2.5	Alle Anwendungs- und Systemkonten und verwandte Zugriffsrechte werden wie folgt zugewiesen und verwaltet: • Basierend auf den geringsten Berechtigungen, die für die Betriebsfähigkeit des Systems oder der Anwendung erforderlich sind. • Der Zugriff ist auf die Systeme, Anwendungen oder Prozesse beschränkt, die ihre Verwendung ausdrücklich erfordern.	• Richtlinien und Prozeduren untersuchen. • Mit System- und Anwendungskonten zugeordnete Privilegien untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
7.2.5.1	Jeder Zugriff von Anwendungs- und Systemkonten und verwandten Zugriffsprivilegien werden wie folgt überprüft: • Regelmäßig (in der Häufigkeit, die in der gezielten Risikoanalyse der Entität definiert ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird. • Der Anwendungs-/Systemzugriff bleibt für die durchgeführte Funktion angemessen. • Jeder unangemessene Zugriff wird adressiert. • Die Verwaltung bestätigt, dass der Zugriff weiterhin angemessen ist.	• Richtlinien und Prozeduren untersuchen. • Die gezielte Risikoanalyse untersuchen. • Verantwortliches Personal befragen. • Dokumentierte Ergebnisse von regelmäßigen Überprüfungen von System- und Anwendungskonten und verwandte Privilegien untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
7.2.6	Jeglicher Benutzerzugriff auf Abfrage-Repositorien von gespeicherter Karteninhaberdaten ist wie folgt beschränkt: • Über Anwendungen oder andere programmatische Methoden, mit Zugriff und zulässigen Aktionen basierend auf Benutzerrollen und geringsten Privilegien. • Nur der/die verantwortliche(n) Administrator(en) kann/können direkt auf Repositorien gespeicherter CHD zugreifen oder diese abfragen.	• Richtlinien und Prozeduren untersuchen. • Personal befragen. • Konfigurationseinstellungen zum Abfragen von Repositorien von gespeicherten Karteninhaberdaten untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für Kontrollen für den Benutzerzugriff auf Abfrage-Repositorien gespeicherter Karteninhaberdaten. Siehe Anforderungen 7.2.5 und 7.2.5.1 und 8.6.1 bis 8.6.3 für Kontrollen für Anwendungs- und Systemkonten.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
7.3 Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsystem(e) verwaltet.							
7.3.1	Ein oder mehrere Zugriffskontrollsysteme sind vorhanden, die den Zugriff basierend auf den Informationsbedürfnissen eines Benutzers einschränken und alle Systemkomponenten abdecken.	• Anbieterdokumentation untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
7.3.2	Das/die Zugriffskontrollsystem(e) ist/sind so konfiguriert, dass es Berechtigungen erzwingt, die Personen, Anwendungen, und Systemen basierend auf Jobklassifizierung und Funktion zugewiesen wurden.	• Anbieterdokumentation untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
7.3.3	Das/die Zutrittskontrollsystem(e) ist/sind standardmäßig auf „Alles verweigern“ eingestellt.	• Anbieterdokumentation untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐

Anforderung 8: Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.1 Prozesse und Mechanismen zur Identifizierung von Benutzern und zur Authentifizierung des Zugriffs auf Systemkomponenten werden definiert und verstanden.							
8.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 8 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
8.1.2	Die Rollen und Zuständigkeiten für die Durchführung der Aktivitäten gemäß Anforderung 8 sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
8.2 Die Benutzeridentifizierung und verwandte Konten für Benutzer und Administratoren werden während des gesamten Lebenszyklus eines Kontos streng verwaltet.							
8.2.1	Allen Benutzern wird eine eindeutige ID zugewiesen, bevor der Zugriff auf Systemkomponenten oder Karteninhaberdaten zugelassen wird.	• Verantwortliches Personal befragen. • Audit-Protokolle und anderen Nachweis untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten im Rahmen von Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen.						

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.2.2	Gruppen-, gemeinsame oder generische IDs, oder andere gemeinsame Authentifizierungs-Anmeldeinformationen werden nur in Ausnahmefällen verwendet und wie folgt verwaltet: • Die Verwendung des IDs wird verhindert, es sei denn, es liegt ein außergewöhnlicher Umstand vor. • Die Verwendung ist auf die für den außergewöhnlichen Umstand erforderliche Zeit beschränkt. • Die geschäftliche Rechtfertigung zur Verwendung wird dokumentiert. • Die Verwendung wird ausdrücklich von der Geschäftsleitung genehmigt. • Die individuelle Benutzeridentität wird bestätigt, bevor der Zugriff auf ein Konto gewährt wird. • Jede durchgeführte Aktion ist einem einzelnen Benutzer zuzuordnen.	• Benutzerkontenlisten auf Systemkomponenten und die entsprechende Dokumentation untersuchen. • Authentifizierungsrichtlinien und -prozeduren untersuchen. • Systemadministratoren befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten im Rahmen von Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen.						
8.2.3	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter***						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.2.4	Das Hinzufügen, Löschen und Ändern von Benutzer-IDs, Authentifizierungsfaktoren, Authentifizierungsfaktoren und anderen Identifiziererobjekten wird wie folgt verwaltet: • Autorisiert mit entsprechender Zulassung. • Implementiert nur mit den Privilegien, die in der dokumentierten Genehmigung angegeben sind.	• Dokumentierte Autorisierungen in verschiedenen Phasen des Kontolebenszyklus (Hinzufügungen, Änderungen und Löschungen) untersuchen. • Systemeinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Benutzerkonten, einschließlich Mitarbeiter, Auftragnehmer, Berater, Zeitarbeiter und Drittanbieter.						
8.2.5	Der Zugriff für gekündigte Benutzer wird sofort widerrufen.	• Informationsquellen für gekündigte Benutzer untersuchen. • Die aktuellen Benutzerzugriffslisten überprüfen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
8.2.6	Inaktive Benutzerkonten werden innerhalb von 90 Tagen nach Inaktivität entfernt oder deaktiviert.	• Benutzerkonten und letzte Anmeldeinformationen untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
8.2.7	Konten, die von Dritten verwendet werden, um per Fernzugriff auf Systemkomponenten zuzugreifen, sie zu unterstützen oder zu warten, werden wie folgt verwaltet: • Nur während des erforderlichen Zeitraums aktiviert, und deaktiviert, wenn sie nicht verwendet werden. • Die Verwendung wird auf unerwartete Aktivitäten überwacht.	• Verantwortliches Personal befragen. • Dokumentation zur Verwaltung von Konten untersuchen. • Nachweis untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.2.8	Wenn eine Benutzersitzung länger als 15 Minuten inaktiv war, muss sich der Benutzer erneut authentifizieren, um das Terminal oder die Sitzung erneut zu aktivieren.	• Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen. Diese Anforderung soll nicht verhindern, dass legitime Aktivitäten durchgeführt werden, während die Konsole/der PC unbeaufsichtigt ist.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.3 Starke Authentifizierung für Benutzer und Administratoren wird etabliert und verwaltet.							
8.3.1	Der gesamte Benutzerzugriff auf Systemkomponenten für Benutzer und Administratoren wird über mindestens einen der folgenden Authentifizierungsfaktoren authentifiziert: • Etwas, das Sie wissen, wie ein Passwort oder eine Passphrase. • Etwas, das Sie besitzen, wie ein Token-Gerät oder eine Smartcard. • Etwas Persönliches, wie ein biometrisches Element.	• Dokumentation, die den/die verwendeten Authentifizierungsfaktor (en) beschreibt/beschreiben, untersuchen. • Für jede Art von Authentifizierungsfaktor, der mit jeder Systemkomponentenart verwendet wird, den Authentifizierungsprozess beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen. Diese Anforderung ersetzt nicht die Anforderungen an die mehrstufige Authentifizierung (MFA), gilt jedoch für die im Geltungsbereich enthaltenen Systeme, die ansonsten nicht den MFA-Anforderungen unterliegen. Ein digitales Zertifikat ist eine gültige Option für „etwas, das Sie besitzen“, wenn es für einen bestimmten Benutzer eindeutig ist						
8.3.2	Starke Kryptografie wird verwendet, um alle Authentifizierungsfaktoren während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar zu machen.	• Anbieterdokumentation untersuchen • Systemkonfigurationseinstellungen untersuchen. • Repositorien von Authentifizierungsfaktoren untersuchen. • Datenübertragungen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.3.3	Die Benutzeridentität wird verifiziert, bevor ein Authentifizierungsfaktor geändert wird.	• Prozeduren zum Modifizieren von Authentifizierungsfaktoren untersuchen. • Sicherheitspersonal beachten.	☐	☐	☐	☐	☐
8.3.4	Ungültige Authentifizierungsversuche werden eingeschränkt durch: • Sperren der Benutzer-ID nach nicht mehr als 10 Versuchen. • Einstellen der Sperrdauer auf mindestens 30 Minuten oder bis die Identität des Benutzers bestätigt ist.	• Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten im Rahmen von Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen.						
8.3.5	Wenn Passwörter/Passphrasen als Authentifizierungsfaktoren verwendet werden, um Anforderung 8.3.1 zu erfüllen, dann werden sie für jeden Benutzer wie folgt eingestellt und neu eingestellt: • Einstellung auf einen eindeutigen Wert für die erstmalige Verwendung und bei Neueinstellung. • Muss sofort nach der ersten Verwendung geändert werden.	• Prozeduren zum Einstellen und Neu Einstellen von Passwörtern/Passphrasen untersuchen. • Sicherheitspersonal beachten.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.3.6	Wenn Passwörter/Passphrasen als Authentifizierungsfaktoren verwendet werden, um Anforderung 8.3.1 zu erfüllen, erfüllen sie die folgende Mindestkomplexitätsebene: • Eine Mindestlänge von 12 Zeichen (oder wenn das System 12 Zeichen nicht unterstützt, eine Mindestlänge von acht Zeichen). • Enthält sowohl numerische als auch alphabetische Zeichen.	• Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt nicht für: • Benutzerkonten an Kassenterminals, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen. • Anwendungs- oder Systemkonten, die den Anforderungen in Abschnitt 8.6 unterliegen. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.* Bis zum 31. März 2025 müssen Passwörter gemäß PCI DSS v3.2.1 Anforderung 8.2.3 eine Mindestlänge von sieben Zeichen aufweisen.						
8.3.7	Personen ist es nicht gestattet, ein neues Passwort/eine neue Passphrase vorzulegen, das/die mit den letzten vier verwendeten Passwörtern/Passwörtern identisch ist.	• Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten im Rahmen von Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.3.8	Authentifizierungsrichtlinien und -prozeduren werden dokumentiert und allen Benutzern mitgeteilt, einschließlich: • Anleitungen zur Auswahl von starken Authentifizierungsfaktoren. • Anleitungen, wie Benutzer ihre Authentifizierungsfaktoren schützen sollten. • Anweisungen, zuvor verwendete Passwörter/Passphrasen nicht wiederzuverwenden. • Anweisungen zum Ändern von Passwörtern/Passphrasen bei Verdacht oder Wissen, dass das Passwort/die Passphrasen kompromittiert wurden und wie der Vorfall zu melden ist.	• Prozeduren untersuchen. • Personal befragen. • Authentifizierungsrichtlinien und -verfahren, die an die Benutzer verteilt werden, überprüfen. • Benutzer befragen.	☐	☐	☐	☐	☐
8.3.9	Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Benutzerzugriff verwendet werden (d. h. in einer Implementierung der Single-Faktor-Authentifizierung), dann entweder: • Passwörter/Passphrasen werden mindestens alle 90 Tage geändert, **ODER** • Die Sicherheitshaltung von Konten wird dynamisch analysiert und der Echtzeitzugriff auf Ressourcen wird entsprechend automatisch bestimmt. *(fortgesetzt)*	• Systemkonfigurationseinstellungen inspizieren.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
	Hinweise zur Anwendbarkeit Diese Anforderung gilt nicht für im Geltungsbereich enthaltene Systemkomponenten, wo MFA verwendet wird. Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen. Diese Anforderung gilt nicht für Kundenkonten von Dienstleistungsanbietern, jedoch für Konten für Personal von Dienstleistungsanbietern.						
8.3.10	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter***						
8.3.10.1	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter***						
8.3.11	Wenn Authentifizierungsfaktoren wie physische oder logische Sicherheitstoken, Smartcards oder Zertifikate verwendet werden, dann: • werden Faktoren einem einzelnen Benutzer zugewiesen und nicht von mehreren Benutzern geteilt. • stellen physische und/oder logische Kontrollen sicher, dass nur der beabsichtigte Benutzer diesen Faktor verwenden kann, um Zugriff zu erhalten.	• Authentifizierungsrichtlinien und -prozeduren untersuchen. • Sicherheitspersonal befragen. • Systemkonfigurationseinstellungen untersuchen und/oder gegebenenfalls physische Kontrollen beachten.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.4 Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern.							
8.4.1	MFA wird für alle Nicht-Konsolen-Zugriffe auf die CDE für Personal mit administrativem Zugriff implementiert.	• Netzwerk- und/oder Systemkonfigurationen untersuchen. • Das Administratorpersonal, das sich bei der CDE anmeldet, beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Die Anforderung für MFA für den Nicht-Konsolen-Administratorzugriff gilt für jedes Personal mit erhöhten oder gesteigerten Rechten, die über eine Nicht-Konsolen-Verbindung auf die CDE zugreifen, d. h. über einen logischen Zugriff, der über eine Netzwerkschnittstelle statt über eine direkte, physische Verbindung erfolgt.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.4.2	MFA ist für alle Nicht-Konsolen-Zugriffe auf die CDE implementiert.	• Netzwerk- und/oder Systemkonfigurationen untersuchen. • Das Personal beachten, das sich bei der CDE anmeldet. • Nachweis untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Diese Anforderung gilt nicht für: • Anwendungs- oder Systemkonten, die automatisierte Funktionen durchführen. • Benutzerkonten an Kassenterminals, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen. • Benutzerkonten, die nur mit Phishing-resistenten Authentifizierungsfaktoren authentifiziert sind. MFA ist für beide Zugriffsarten erforderlich, die in den Anforderungen 8.4.2 und 8.4.3 angegeben sind. Daher ersetzt die Anwendung von MFA auf einen Zugriffstyp nicht die Notwendigkeit, eine andere Instanz von MFA auf den anderen Zugriffstyp anzuwenden. Wenn sich eine Person zuerst per Fernzugriff mit dem Netzwerk der Entität verbindet und später eine Verbindung zur CDE aus dem Netzwerk heraus initiiert, würde sich die Person gemäß dieser Anforderung zweimal unter Verwendung von MFA authentifizieren, einmal bei der Verbindung über Fernzugriff auf das Netzwerk der Entität und einmal bei der Verbindung aus dem Netzwerk der Entität in die CDE. Die MFA-Anforderungen gelten für alle Arten von Systemkomponenten, einschließlich Cloud, gehostete Systeme und lokale Anwendungen, Netzwerksicherheitsgeräte, Arbeitsstationen, Server und Endpunkte und umfassen den direkten Zugriff auf die Netzwerke oder Systeme einer Entität sowie webbasierten Zugriff auf eine Anwendung oder Funktion. MFA für den Zugriff auf die CDE kann auf Netzwerk- oder System-/Anwendungsebene implementiert werden; sie muss nicht auf beiden Ebenen angewendet werden. Wenn zum Beispiel MFA verwendet wird, wenn sich ein Benutzer mit dem CDE-Netzwerk verbindet, muss es nicht verwendet werden, wenn sich der Benutzer bei jedem System oder jeder Anwendung innerhalb der CDE anmeldet. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.4.3	MFA wird für alle Fern-Zugriffe von außerhalb des Netzwerks der Entität, die auf die CDE zugreifen oder diese beeinflussen könnten, implementiert.	• Netzwerk- und/oder Systemkonfigurationen für Server und Systeme mit Fernzugriff untersuchen. • Das Personal (zum Beispiel Benutzer und Administratoren), das sich per Fernzugriff mit dem Netzwerk verbindet, beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Die Anforderung an MFA für Fernzugriff von außerhalb des Netzwerks der Entität gilt für alle Benutzerkonten, die aus der Ferne auf das Netzwerk zugreifen können, wobei dieser Fernzugriff zu einem Zugriff auf die CDE führt oder führen könnte. Dazu gehören alle Fernzugriffe von Personal (Benutzern und Administratoren) und Dritten (einschließlich, aber nicht beschränkt auf Verkäufer, Lieferanten, Dienstleister und Kunden). Wenn der Fernzugriff auf einen Teil des Netzwerks der Entität erfolgt, das ordnungsgemäß von der CDE segmentiert ist, sodass Fernbenutzer nicht auf die CDE zugreifen oder diese beeinflussen können, ist MFA für den Fernzugriff auf diesen Teil des Netzwerks nicht erforderlich. MFA ist jedoch für jeden Fernzugriff auf Netzwerke mit Zugriff auf die CDE erforderlich und wird für alle Fernzugriffe auf die Netzwerke der Entität empfohlen. Die MFA-Anforderungen gelten für alle Arten von Systemkomponenten, einschließlich Cloud, gehostete Systeme und lokale Anwendungen, Netzwerksicherheitsgeräte, Arbeitsstationen, Server und Endpunkte und umfassen den direkten Zugriff auf die Netzwerke oder Systeme einer Entität sowie webbasierten Zugriff auf eine Anwendung oder Funktion.					

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.5 Multi-Faktor-Authentifizierungssysteme (MFA) sind so konfiguriert, dass sie Missbrauch verhindern.							
8.5.1	MFA-Systeme werden wie folgt implementiert: • Das MFA-System ist nicht für Wiederholungsangriffe anfällig. • MFA-Systeme können von Benutzern, einschließlich Administratoren, nicht umgangen werden, es sei denn, dies ist ausdrücklich dokumentiert und ausnahmsweise für einen begrenzten Zeitraum von der Verwaltung autorisiert. • Es werden mindestens zwei verschiedene Arten von Authentifizierungsfaktoren verwendet. • Der Erfolg aller Authentifizierungsfaktoren ist erforderlich, bevor der Zugriff gewährt wird.	• Anbietersystemdokumentation untersuchen. • Systemkonfigurationen für die MFA-Implementierung untersuchen. • Verantwortliches Personal befragen und Prozesse beachten. • Personal beachten, das sich in Systemkomponenten in der CDE anmeldet. • Personal beachten, das sich aus der Ferne von außerhalb des Netzwerks der Entität verbindet.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.6 Die Verwendung von Anwendungs- und Systemkonten und zugeordneten Authentifizierungsfaktoren wird streng verwaltet.							
8.6.1	Wenn Konten, die von Systemen oder Anwendungen verwendet werden, für die interaktive Anmeldung verwendet werden können, werden diese wie folgt verwaltet: • Interaktive Verwendung wird verhindert, es sei denn, es liegt ein außergewöhnlicher Umstand vor. • Interaktive Verwendung ist auf die für den außergewöhnlichen Umstand erforderliche Zeit beschränkt. • Die geschäftliche Rechtfertigung zur interaktiven Verwendung wird dokumentiert. • Interaktive Verwendung wird ausdrücklich von der Geschäftsleitung genehmigt. • Die individuelle Benutzeridentität wird bestätigt, bevor der Zugriff auf das Konto gewährt wird. • Jede durchgeführte Aktion ist einem einzelnen Benutzer zuzuordnen.	• Anwendungs- und Systemkonten untersuchen, die für eine interaktive Anmeldung verwendet werden können. • Administratives Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
8.6.2	Passwörter/Passphrasen für alle Anwendungs- und Systemkonten, die für die interaktive Anmeldung verwendet werden können, sind nicht in Skripten, Konfigurations-/Eigenschaftsdateien oder maßgeschneidertem und benutzerdefiniertem Quellcode fest codiert.	• Personal befragen. • Systementwicklungsprozeduren untersuchen. • Skripte, Konfigurations-/Eigenschaftsdateien und maßgeschneiderten und benutzerdefinierten Quellcode für Anwendungs- und Systemkonten, die für die interaktive Anmeldung verwendet werden können, untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Gespeicherte Passwörter/Passphrasen müssen gemäß PCI DSS-Anforderung 8.3.2 verschlüsselt werden. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
8.6.3	Passwörter/Passphrasen für beliebige Anwendungs- und Systemkonten werden wie folgt gegen Missbrauch geschützt: • Passwörter/Passphrasen werden regelmäßig geändert (in der Häufigkeit, die in der gezielten Risikoanalyse der Entität festgelegt ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird) und bei Verdacht oder Bestätigung einer Kompromittierung. • Passwörter/Passphrasen sind mit ausreichender Komplexität aufgebaut, entsprechend wie häufig die Entität die Passwörter/Passphrasen ändert.	• Richtlinien und Prozeduren untersuchen. • Die gezielte Risikoanalyse untersuchen. • Verantwortliches Personal befragen. • Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.1 Prozesse und Mechanismen zur Einschränkung des physischen Zugriffs auf Karteninhaberdaten werden definiert und verstanden.							
9.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 9 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
9.1.2	Die Rollen und Zuständigkeiten für die Durchführung der Aktivitäten gemäß Anforderung 9 sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
9.2 Physische Zugriffskontrollen verwalten den Zutritt zu Einrichtungen und Systemen, die Karteninhaberdaten enthalten.							
9.2.1	Geeignete Zugangskontrollen für Einrichtungen sind vorhanden, um den physischen Zugriff auf Systeme in der CDE einzuschränken.	• Physische Eintrittskontrollen beachten. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt nicht für Standorte, die von Verbrauchern (Karteninhabern) öffentlich zugänglich sind.						

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.2.1.1	Der individuelle physische Zugriff zu sensiblen Bereichen innerhalb der CDE wird entweder mit Videokameras oder physischen Zugriffskontrollmechanismen (oder beidem) wie folgt überwacht: • Ein- und Austrittspunkte zu/aus sensiblen Bereichen innerhalb der CDE werden überwacht. • Überwachungsgeräte oder -mechanismen sind vor Manipulation oder Deaktivierung geschützt. • Gesammelte Daten werden überprüft und mit anderen Einträgen korreliert. • Gesammelte Daten werden für mindestens drei Monate gespeichert, sofern nicht anders gesetzlich eingeschränkt.	• Standorte beachten, an denen individueller physischer Zugriff auf sensiblen Bereichen innerhalb der CDE erfolgt. • Die physischen Zugriffskontrollmechanismen beachten und/oder Videokameras untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
9.2.2	Physische und/oder logische Kontrollen werden implementiert, um die Verwendung von öffentlich zugänglichen Netzwerkbuchsen innerhalb der Einrichtung einzuschränken.	• Verantwortliches Personal befragen. • Standorte von öffentlich zugänglichen Netzwerkbuchsen beachten.	☐	☐	☐	☐	☐
9.2.3	Der physische Zugriff auf drahtlose Zugriffspunkten, Gateways, Netzwerk-/Kommunikationshardware und Telekommunikationsleitungen innerhalb der Einrichtung ist eingeschränkt.	• Verantwortliches Personal befragen. • Standorte von Hardware und Leitungen beachten.	☐	☐	☐	☐	☐
9.2.4	Der Zugriff auf Konsolen in sensiblen Bereichen ist bei Nichtverwendung durch eine Sperre eingeschränkt.	• Den Versuch eines Systemadministrators beachten, sich bei Konsolen in sensiblen Bereichen anzumelden.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.3 Der physische Zugriff für Personal und Besucher wird autorisiert und verwaltet.							
9.3.1	Es werden Prozeduren zur Autorisierung und Verwaltung des physischen Zugriffs von Personal auf die CDE implementiert, einschließlich: • Identifizierung von Personal. • Verwaltung von Änderungen der physischen Zugriffsanforderungen einer Person. • Widerruf oder Beendigung der Personalidentifizierung. • Beschränkung des Zugriffs auf den Identifizierungsprozess oder -system auf autorisiertes Personal.	• Dokumentierte Prozeduren untersuchen. • Identifizierungsmethoden, wie ID-Abzeichen beachten. • Prozesse beachten.	☐	☐	☐	☐	☐
9.3.1.1	Der physische Zugriff auf sensible Bereiche innerhalb der CDE für das Personal wird wie folgt kontrolliert: • Der Zugriff ist autorisiert und basiert auf der individuellen Jobfunktion. • Der Zugriff wird nach Beendigung sofort entzogen. • Alle physischen Zugriffsmechanismen wie Schlüssel, Zugriffskarten usw. werden bei Beendigung zurückgegeben oder deaktiviert.	• Personal in sensiblen Bereichen innerhalb der CDE beachten. • Verantwortliches Personal befragen. • Physische Zugriffskontrolllisten untersuchen. • Prozesse beachten.	☐	☐	☐	☐	☐
9.3.2	Es werden Prozeduren zur Autorisierung und Verwaltung von Besucherzugriffs auf die CDE implementiert, einschließlich: • Besucher werden vor dem Betreten autorisiert. • Besucher werden jederzeit begleitet. • Besucher werden eindeutig identifiziert und erhalten ein Abzeichen oder eine andere Identifizierung, die abläuft. • Besucherabzeichen oder andere Identifizierungsmerkmale unterscheiden Besucher sichtbar vom Personal.	• Dokumentierte Prozeduren untersuchen. • Prozesse beachten, wenn Besucher in der CDE anwesend sind. • Personal befragen. • die Verwendung von Besucherabzeichen oder anderen Identifizierungen beachten.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.3.3	Besucherabzeichen oder -identifizierungen werden vor Verlassen der Anlage oder zum Ablaufdatum abgegeben bzw. deaktiviert.	• Besucher beachten, die die Einrichtung verlassen. • Personal befragen.	☐	☐	☐	☐	☐
9.3.4	Besucherprotokoll werden verwendet, um eine physische Aufzeichnung der Besucheraktivitäten innerhalb der Einrichtung und in sensiblen Bereichen zu führen, einschließlich: • Den Namen des Besuchers und die vertretene Organisation. • Datum und Uhrzeit des Besuchs. • Der Name des Personals, das den physischen Zugang autorisiert. • Aufbewahrung des Protokolls für mindestens drei Monate, sofern nicht anders gesetzlich eingeschränkt.	• Die Besucherprotokolle untersuchen. • Verantwortliches Personal befragen. • Speicherstandorte für Besucherprotokolle.	☐	☐	☐	☐	☐
9.4 Medien mit Karteninhaberdaten werden sicher gespeichert, darauf zugegriffen, verteilt und vernichtet.							
9.4.1	Alle Medien mit Karteninhaberdaten werden physisch gesichert.	• Dokumentation untersuchen.	☐	☐	☐	☐	☐
9.4.1.1	Offline-Medien-Backups mit Karteninhaberdaten werden an einem sicheren Ort gespeichert.	• Dokumentierte Prozeduren untersuchen. • Protokolle oder andere Dokumentation untersuchen. • Verantwortliches Personal an dem/den Speicherort(en) befragen.	☐	☐	☐	☐	☐
9.4.1.2	Die Sicherheit des/der Offline-Medien-Backup-Standorte(s) mit Karteninhaberdaten wird mindestens alle 12 Monate überprüft.	• Dokumentierte Prozeduren, Protokolle oder andere Dokumentation untersuchen. • Verantwortliches Personal an dem/den Speicherstandort(en) befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.4.2	Alle Medien mit Karteninhaberdaten werden gemäß der Sensibilität der Daten klassifiziert.	• Dokumentierte Prozeduren untersuchen. • Medienprotokolle oder andere Dokumentation untersuchen.	☐	☐	☐	☐	☐
9.4.3	Außerhalb der Einrichtung versendete Medien mit Karteninhaberdaten werden wie folgt gesichert: • Außerhalb der Einrichtung gesendete Medien werden protokolliert. • Die Medien werden per gesichertem Kurier oder einer anderen Zustellmethode versandt, die genau nachverfolgt werden kann. • Offsite-Verfolgungs-Protokolle enthalten Details zum Medienstandort.	• Dokumentierte Prozeduren untersuchen. • Personal befragen. • Aufzeichnungen untersuchen. • Offsite-Verfolgungsprotokolle für alle Medien untersuchen.	☐	☐	☐	☐	☐
9.4.4	Das Management genehmigt alle Medien mit Karteninhaberdaten, die außerhalb der Einrichtung bewegt werden (einschließlich der Verteilung von Medien an Personen).	• Dokumentierte Prozeduren untersuchen. • Offsite-Medien-Verfolgungsprotokolle untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Personen, die Medienbewegungen genehmigen, sollten über die entsprechende Verwaltungsautorität verfügen, um diese Genehmigung zu gewähren. Es ist jedoch nicht ausdrücklich erforderlich, dass diese Personen „Verwalter“ als Teil ihres Titels haben.						
9.4.5	Inventarprotokolle aller elektronischen Medien mit Karteninhaberdaten werden geführt.	• Dokumentierte Prozeduren untersuchen. • Inventarprotokolle für elektronische Medien untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.4.5.1	Inventare elektronischer Medien mit Karteninhaberdaten werden mindestens alle 12 Monate durchgeführt.	• Dokumentierte Prozeduren untersuchen. • Inventarprotokolle für elektronische Medien untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
9.4.6	Gedruckte Materialien mit Karteninhaberdaten werden, wenn sie aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, wie folgt vernichtet: • Die Materialien werden quergeschnitten, zerkleinert, verbrannt oder eingestampft, sodass Karteninhaberdaten nicht rekonstruiert werden können. • Materialien werden vor der Vernichtung in sicheren Speichercontainern gespeichert.	• Die Richtlinie zur Medienvernichtung untersuchen. • Prozesse beachten. • Personal befragen. • Speichercontainer beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderungen an die Vernichtung von Medien, wenn diese Medien aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, sind getrennt und unterscheiden sich von PCI DSS-Anforderung 3.2.1, die das sichere Löschen von Karteninhaberdaten betrifft, wenn sie gemäß den Karteninhaberdaten-Aufbewahrungsrichtlinien der Entität nicht mehr benötigt werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.4.7	Elektronische Medien mit Karteninhaberdaten werden, wenn sie aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, auf eine der folgenden Weisen vernichtet: • Die elektronischen Medien werden vernichtet. • Die Karteninhaberdaten werden unwiederbringlich gemacht, sodass sie nicht rekonstruiert werden können.	• Die Richtlinie zur Medienvernichtung untersuchen. • Der Prozess der Medienvernichtung beachten. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderungen an die Vernichtung von Medien, wenn diese Medien aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, sind getrennt und unterscheiden sich von PCI DSS-Anforderung 3.2.1, die das sichere Löschen von Karteninhaberdaten betrifft, wenn sie gemäß den Karteninhaberdaten-Aufbewahrungsrichtlinien der Entität nicht mehr benötigt werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.5 Interaktionspunkt- (POI)-Geräte sind vor Manipulation und nicht autorisiertem Austausch geschützt.							
9.5.1	POI-Geräte, die Zahlungskartendaten durch direkte physische Interaktion mit dem Zahlungskartenformfaktor erfassen, sind vor Manipulation und nicht autorisiertem Austausch geschützt, einschließlich der folgenden: • Führen einer Liste von POI-Geräten. • Regelmäßiges Inspizieren von POI-Geräten auf Manipulation oder nicht autorisierten Austausch. • Schulung des Personals, um verdächtiges Verhalten zu erkennen und Manipulationen oder nicht autorisierten Austausch von Geräten zu melden.	• Dokumentierte Richtlinien und Prozeduren untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderungen gelten für eingesetzte POI-Geräte, die bei Transaktionen mit vorhandener Karte verwendet werden (d. h. einen Zahlungskartenformfaktor wie eine Karte, die durchgezogen, angetippt oder eingetaucht wird). Diese Anforderungen gelten nicht für: • Komponenten, die nur für manuelle PAN-Schlüsseleingabe verwendet werden. • Kommerzielle Standardgeräte (COTS) (zum Beispiel Smartphones oder Tablets), die mobile Geräte im Besitz von Händlern sind, die für den Massenmarkt bestimmt sind.						
9.5.1.1	Es wird eine aktuelle Liste von POI-Geräten geführt, einschließlich: • Marke und Modell des Geräts. • Standort des Geräts. • Seriennummer des Geräts oder andere Methoden zur eindeutigen Identifizierung.	• Die Liste von POI-Geräten untersuchen. • POI-Geräte und Gerätestandorte beachten. • Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
9.5.1.2	Die Oberflächen von POI-Geräten werden regelmäßig inspiziert, um Manipulationen und nicht autorisierten Austausch zu erkennen.	• Dokumentierte Prozeduren untersuchen. • Verantwortliches Personal befragen. • Inspizierungsprozesse beachten.	☐	☐	☐	☐	☐
9.5.1.2.1	Die Häufigkeit der regelmäßigen Inspektionen von POI-Geräten und die Art der durchgeführten Inspektionen wird in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	• Die gezielte Risikoanalyse untersuchen. • Dokumentierte Ergebnisse von regelmäßigen Geräteinspektionen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
9.5.1.3	Das Personal in POI-Umgebungen wird geschult, um auf Manipulationsversuche oder den Ersatz von POI-Geräten aufmerksam zu machen, und umfasst: • Verifizierung der Identität von Drittpersonen, die sich als Reparatur- oder Wartungspersonal ausgeben, bevor ihnen Zugriff zum Modifizieren oder Beheben von Fehlern von Geräten gewährt wird. • Prozeduren, um sicherzustellen, dass Geräte ohne Verifizierung nicht installiert, ersetzt oder zurückgegeben werden. • Sich verdächtigen Verhaltens in der Nähe von Geräten bewusst zu sein. • Melden von verdächtigem Verhalten und Hinweisen auf Gerätemanipulation oder Austausch an das entsprechende Personal.	• Schulungsmaterialien für Personal in POI-Umgebungen überprüfen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

Regelmäßige Überwachung und Prüfung der Netzwerke

Anforderung 10: Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.1 Prozesse und Mechanismen zur Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten werden definiert und verstanden.							
10.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 10 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
10.1.2	Die Rollen und Verantwortlichkeiten für die Durchführung der in Anforderung 10 genannten Aktivitäten sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
10.2 Audit-Protokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten, und die forensische Analyse von Ereignissen zu unterstützen.							
10.2.1	Audit-Protokolle sind für alle Systemkomponenten und Karteninhaberdaten aktiviert und aktiv.	• Den Systemadministrator befragen. • Systemkonfigurationen untersuchen.	☐	☐	☐	☐	☐
10.2.1.1	Audit-Protokolle erfassen alle individuellen Benutzerzugriffe auf Karteninhaberdaten.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.2.1.2	Audit-Protokolle erfassen alle Aktionen, die von einer Person mit Administratorzugriff ausgeführt werden, einschließlich der interaktiven Verwendung von Anwendungs- oder Systemkonten.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐
10.2.1.3	Audit-Protokolle erfassen den gesamten Zugriff auf Audit-Protokolle.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐
10.2.1.4	Audit-Protokolle erfassen alle ungültigen logischen Zugriffsversuche.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐
10.2.1.5	Audit-Protokolle erfassen alle Änderungen an Identifizierungs- und Authentifizierungsreferenzen einschließlich, aber nicht beschränkt auf: • Erstellung neuer Konten. • Erhöhung der Privilegien. • Alle Änderungen, Ergänzungen oder Löschungen von Konten mit Administratorzugriff.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐
10.2.1.6	Audit-Protokolle erfassen Folgendes: • Alle Initialisierungen neuer Audit-Protokolle, und • Alles Starten, Stoppen oder Pausieren der bestehenden Audit-Protokolle.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐
10.2.1.7	Audit-Protokolle erfassen die gesamte Erstellung und Löschung von Objekten auf Systemebene.	• Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.2.2	Audit-Protokolle zeichnen die folgenden Details für jedes auditierbare Ereignis auf: • Benutzeridentifizierung. • Art des Vorkommnisses. • Datum und Uhrzeit. • Erfolgs- und Versagensanzeige. • Entstehung des Vorkommnisses. • Identität oder Name der betroffenen Daten, Systemkomponente, Ressource oder der Dienstleistung (zum Beispiel Name und Protokoll).	• Verantwortliches Personal befragen. • Audit-Protokollkonfigurationen untersuchen. • Audit-Protokolldaten untersuchen.	☐	☐	☐	☐	☐
10.3 Audit-Protokolle werden vor Vernichtung und nicht autorisierten Änderungen geschützt.							
10.3.1	Der Lesezugriff auf Audit-Protokoll-Dateien ist auf Personen mit berufsbedingtem Bedarf beschränkt.	• Systemadministratoren befragen • Systemkonfigurationen und Privilegien untersuchen.	☐	☐	☐	☐	☐
10.3.2	Audit-Protokoll-Dateien sind geschützt, um Änderungen durch Personen zu verhindern.	• Systemkonfigurationen und Privilegien untersuchen. • Systemadministratoren befragen.	☐	☐	☐	☐	☐
10.3.3	Audit-Protokoll-Dateien, auch für nach außen gerichtete Technologien, werden zeitnah auf einem sicheren, zentralen, internen Protokollserver oder anderen schwer veränderbaren Medien gesichert.	• Backup-Konfigurationen oder Protokolldateien untersuchen.	☐	☐	☐	☐	☐
10.3.4	Dateiintegritätsüberwachung oder Änderungserkennungsmechanismen werden auf Audit-Protokollen verwendet, um sicherzustellen, dass vorhandene Protokolldaten nicht geändert werden können, ohne dass Warnungen generiert werden.	• Systemeinstellungen untersuchen. • Überwachte Dateien untersuchen. • Ergebnisse der Überwachungsaktivitäten untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.4 Audit-Protokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren.							
10.4.1	Die folgenden Audit-Protokolle werden mindestens einmal täglich überprüft: • Alle Sicherheitsereignisse. • Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen. • Protokolle aller kritischen Systemkomponenten. • Protokolle aller Server und Systemkomponenten, die Sicherheitsfunktionen durchführen (zum Beispiel Netzwerksicherheitskontrollen, Eindringungs-Erkennungs-Systeme/Eindringungs-Verhinderungs-Systeme (IDS/IPS), Authentifizierungsserver).	• Sicherheitsrichtlinien und Prozeduren untersuchen. • Prozesse beachten. • Personal befragen.	☐	☐	☐	☐	☐
10.4.1.1	Automatisierte Mechanismen werden verwendet, um Audit-Protokoll-Überprüfungen durchzuführen.	• Protokoll-Überprüfungsmechanismen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.4.2	Protokolle aller anderen Systemkomponenten (die nicht in Anforderung 10.4.1 angegeben sind) werden regelmäßig überprüft.	• Sicherheitsrichtlinien und Prozeduren untersuchen. • Dokumentierte Ergebnisse von Protokollüberprüfungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Diese Anforderung gilt für alle anderen in den Geltungsbereich fallenden Systemkomponenten, die nicht in Anforderung 10.4.1 enthalten sind.						
10.4.2.1	Die Häufigkeit der regelmäßigen Protokollüberprüfungen für alle anderen Systemkomponenten (nicht in Anforderung 10.4.1 definiert) wird in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird	• Die gezielte Risikoanalyse untersuchen. • Dokumentierte Ergebnisse von regelmäßigen Protokollüberprüfungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.						
10.4.3	Ausnahmen und Anomalien, die während des Überprüfungsprozesses etabliert wurden, werden adressiert.	• Sicherheitsrichtlinien und Prozeduren untersuchen. • Prozesse beachten. • Personal befragen.	☐	☐	☐	☐	☐
10.5 Der Verlauf des Audit-Protokolls wird gespeichert und steht für Analysen zur Verfügung.							
10.5.1	Den Audit-Protokoll-Verlauf mindestens 12 Monate aufbewahren, wobei mindestens die letzten drei Monate sofort zur Analyse verfügbar sind.	• Dokumentierte Audit-Protokoll-Aufbewahrungs-Richtlinien und Prozeduren untersuchen. • Konfigurationen des Audit-Protokollverlaufs untersuchen. • Audit-Protokolle untersuchen. • Personal befragen. • Prozesse beachten.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.6 Zeitsynchronisierungsmechanismen unterstützen konsistente Zeiteinstellungen über alle Systeme hinweg.							
10.6.1	Systemuhren und Uhrzeit werden mithilfe der Zeitsynchronisierungstechnologie synchronisiert.	• Systemkonfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Um die Zeitsynchronisierungstechnologie auf dem neuesten Stand zu halten, müssen Schwachstellen verwaltet und die Technologie gemäß den PCI-DSS-Anforderungen 6.3.1 und 6.3.3 gepatcht werden.						
10.6.2	Systeme werden wie folgt auf die richtige und konsistente Zeit konfiguriert: • Ein oder mehrere designierte Zeitserver werden verwendet. • Nur der oder die designierten zentralen Zeitserver erhalten die Zeit von externen Quellen. • Die von externen Quellen empfangene Zeit basiert auf der Internationalen Atomzeit oder der koordinierten Weltzeit (UTC). • Der/die designierten Zeitserver akzeptiert/akzeptieren Zeitaktualisierungen nur von bestimmten, von der Branche akzeptierten externen Quellen. • Wenn es mehr als einen designierten Zeitserver gibt, können die Zeitserver sich einander ansehen, um die genaue Zeit beizubehalten. • Interne Systeme erhalten Zeitinformationen nur von bestimmten zentralen Zeitservern.	• Systemkonfigurationseinstellungen zum Erfassen, Verteilen und Speichern der korrekten Zeit untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.6.3	Die Einstellungen und Daten der Zeitsynchronisierung sind wie folgt geschützt: • Der Zugriff auf Zeitdaten ist auf Personal mit geschäftlichem Bedarf beschränkt. • Alle Änderungen der Zeiteinstellungen auf kritischen Systemen werden protokolliert, überwacht und überprüft.	• Systemkonfigurationen und Zeitsynchronisierungseinstellungen und Protokolle untersuchen. • Prozesse beachten.	☐	☐	☐	☐	☐
10.7 Versagen kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und es wird umgehend auf sie reagiert.							
10.7.1	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter***						
10.7.2	Versagen von kritischen Sicherheitskontrollsystemen werden sofort erkannt, gewarnt und adressiert, einschließlich, aber nicht beschränkt auf das Versagen der folgenden kritischen Sicherheitskontrollsysteme: • Netzwerksicherheitskontrollen • IDS/IPS. • Änderungserkennungsmechanismen. • Anti-Malware-Lösungen • Physische Zugriffskontrollen. • Logische Zugriffskontrollen. • Audit-Protokollierungsmechanismen. • Segmentierungskontrollen (sofern verwendet). • Audit-Protokoll-Überprüfungsmechanismen • Automatisierte Sicherheitstesttools (sofern verwendet).	• Dokumentierte Prozesse untersuchen. • Erkennungs- und Alarmierungsprozesse beachten. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Entitäten, einschließlich Dienstleistungsanbieter, und wird Anforderung 10.7.1 vom 31. März 2025 ersetzen. Sie beinhaltet zwei zusätzliche kritische Sicherheitskontrollsysteme, die nicht in Anforderung 10.7.1 enthalten sind. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
10.7.3	Auf Versagen von kritischen Sicherheitskontrollsystemen wird umgehend reagiert, einschließlich, aber nicht beschränkt auf: • Wiederherstellen von Sicherheitsfunktionen. • Identifizieren und Dokumentieren der Dauer (Datum und Uhrzeit von Anfang bis Ende) des Sicherheitsversagens. • Identifizieren und Dokumentieren der Versagensursache(n) und Dokumentieren der erforderlichen Behebung. • Identifizieren und Adressieren von Sicherheitsproblemen, die während des Versagens aufgetreten sind. • Feststellen, ob aufgrund des Sicherheitsversagens weitere Aktionen erforderlich sind. • Implementieren von Kontrollen, um zu verhindern, dass die Versagensursache erneut auftritt. • Wiederaufnehmen der Überwachung der Sicherheitskontrollen.	• Dokumentierte Prozesse untersuchen • Personal befragen. • Aufzeichnungen untersuchen, die sich auf kritische Sicherheitskontrollsystem-Versagen beziehen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die bewertete Entität ein Dienstleistungsanbieter bis 31. März 2025 ist, nach dem diese Anforderung für alle Entitäten gelten wird. *Dies ist eine aktuelle v3.2.1-Anforderung, die nur für Dienstleistungsanbieter gilt. Diese Anforderung ist aber bis zum 31. März 2025 eine bewährte Praktik für alle anderen Entitäten, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

Anforderung 11: Regelmäßige Prüfung der Sicherheit von Systemen und Netzen

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.1 Prozesse und Mechanismen zum regelmäßigen Testen der Sicherheit von Systemen und Netzwerken werden definiert und verstanden.							
11.1.1	Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 11 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
11.1.2	Die Rollen und Zuständigkeiten für die Durchführung der Aktivitäten gemäß Anforderung 11 sind dokumentiert, zugewiesen und verstanden.	• Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.2 Drahtlose Zugriffspunkte werden identifiziert und überwacht, und nicht autorisierte drahtlose Zugriffspunkte werden adressiert.							
11.2.1	Autorisierte und nicht autorisierte drahtlose Zugriffspunkte werden wie folgt verwaltet: • Das Vorhandensein von drahtlosen (Wi-Fi) Zugriffspunkten wird getestet für. • Alle autorisierten und nicht autorisierten drahtlosen Zugriffspunkte werden erkannt und identifiziert. • Testen, Erkennen und Identifizierung findet mindestens einmal alle drei Monate statt. • Wenn automatisierte Überwachung verwendet wird, dann wird das Personal über generierte Warnungen benachrichtigt.	• Richtlinien und Prozeduren untersuchen. • Die angewandte(n) Methodik(en) und die sich ergebende Dokumentation untersuchen. • Personal befragen. • Drahtlose Bewertungsergebnisse untersuchen. • Konfigurationseinstellungen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Die Anforderung gilt selbst dann, wenn eine Richtlinie existiert, die die Verwendung von drahtloser Technologie verbietet. Die zur Erfüllung dieser Anforderung verwendeten Methoden müssen ausreichen, um sowohl autorisierte als auch nicht autorisierte Geräte zu erkennen und zu identifizieren, einschließlich nicht autorisierter Geräte, die an Geräten angeschlossen sind, die selbst autorisiert sind.						
11.2.2	Es wird ein Inventar autorisierter drahtloser Zugriffspunkte geführt, einschließlich einer dokumentierten geschäftlichen Rechtfertigung.	• Dokumentation untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.3 Externe und interne Schwachstellen werden regelmäßig identifiziert, priorisiert und adressiert.							
11.3.1	Interne Schwachstellen-Scans werden wie folgt durchgeführt: • Mindestens einmal alle drei Monate. • Schwachstellen, die entweder risikoreich oder kritisch (gemäß den in Anforderung 6.3.1 definierten Schwachstellenrisiko-Einstufungen der Entität) sind, werden behoben. • Es werden erneute Scans durchgeführt, die bestätigen, dass alle risikoreichen und kritischen Schwachstellen (wie oben erwähnt) behoben wurden. • Das Scan-Tool wird mit den neuesten Schwachstelleninformationen auf dem neuesten Stand gehalten. • Scans werden von qualifiziertem Personal durchgeführt und es besteht organisatorische Unabhängigkeit des Testers.	• Interne Scanbericht-Ergebnisse untersuchen. • Scan-Tool-Konfigurationen untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Es ist nicht erforderlich, einen QSA oder ASV zu verwenden, um interne Schwachstellen-Scans auszuführen. Interne Schwachstellen-Scans können von qualifizierten internen Mitarbeitern durchgeführt werden, die einigermaßen unabhängig von der/den zu scannenden Systemkomponente(n) sind (zum Beispiel sollte ein Netzwerkadministrator nicht für das Scannen des Netzwerks verantwortlich sein), oder eine Entität kann sich dafür entscheiden, interne Schwachstellen-Scans von einer auf Schwachstellen-Scans spezialisierten Firma durchführen zu lassen.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.3.1.1	Alle anderen anwendbaren Schwachstellen (die nicht als risikoreiche Schwachstellen oder kritische Schwachstellen gemäß den Schwachstellenrisikoeinstufungen der Entität, die in Anforderung 6.3.1 definiert sind, eingestuft werden, werden wie folgt verwaltet: • Adressiert basierend auf dem Risiko, das in der gezielten Risikoanalyse der Entität definiert ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird. • Erneute Scans werden nach Bedarf ausgeführt.	• Die gezielte Risikoanalyse untersuchen. • Verantwortliches Personal befragen. • Interne Scanbericht-Ergebnisse oder andere Dokumentation untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Der Zeitrahmen für die Adressierung von Schwachstellen mit geringerem Risiko hängt von den Ergebnissen einer Risikoanalyse gemäß Anforderung 12.3.1 ab, die (mindestens) die Identifizierung von geschützten Assets, Bedrohungen und der Wahrscheinlichkeit und/oder Auswirkung einer Realisierung einer Bedrohung umfasst. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.3.1.2	Interne Schwachstellen-Scans werden über authentifiziertes Scannen wie folgt durchgeführt:						
	• Systeme, die keine Berechtigungsnachweise für authentifiziertes Scannen akzeptieren können, werden dokumentiert.	• Dokumentation untersuchen. • Scan-Tool-Konfigurationen untersuchen. • Scanbericht-Ergebnisse untersuchen. • Personal befragen. • Konten untersuchen, die für authentifiziertes Scannen verwendet werden.	☐	☐	☐	☐	☐
	• Ausreichenden Privilegien werden für solche Systeme verwendet, die Berechtigungsnachweise zum Scannen akzeptieren.		☐	☐	☐	☐	☐
	• Wenn Konten, die für authentifiziertes Scannen verwendet werden, für die interaktive Anmeldung verwendet werden können, dann werden diese gemäß Anforderung 8.2.2 verwaltet.		☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Die authentifizierten Scan-Tools können entweder hostbasiert oder netzwerkbasiert sein. „Ausreichende“ Privilegien sind diejenigen, die für den Zugriff auf Systemressourcen erforderlich sind, damit ein gründlicher Scan durchgeführt werden kann, der bekannte Schwachstellen erkennt. Diese Anforderung gilt nicht für Systemkomponenten, die keine Berechtigungsnachweise zum Scannen akzeptieren können. Beispiele für Systeme, die möglicherweise keine Berechtigungsnachweise zum Scannen akzeptieren, umfassen einige Netzwerk- und Sicherheitsanwendungen, Mainframes und Container. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.3.1.3	Interne Schwachstellen-Scans werden nach jeder bedeutenden Änderung wie folgt durchgeführt: • Schwachstellen, die entweder risikoreich oder kritisch sind (gemäß den in Anforderung 6.3.1 definierten Schwachstellenrisiko-Einstufungen der Entität) werden behoben. • Erneute Scans werden nach Bedarf ausgeführt. • Scans werden von qualifiziertem Personal durchgeführt und es besteht organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	• Änderungskontrolldokumentation untersuchen. • Personal befragen. • Interne Scans untersuchen und gegebenenfalls den Bericht erneut scannen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Ein authentifizierter interner Schwachstellen-Scan gemäß Anforderung 11.3.1.2 ist für Scans, die nach wesentlichen Änderungen durchgeführt werden, nicht erforderlich.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.3.2	Externe Schwachstellen-Scans werden wie folgt durchgeführt: • Mindestens einmal alle drei Monate. • Von einem PCI SSC-zugelassenem Scanning-Anbieter (ASV) • Schwachstellen werden behoben und die Anforderungen des *ASV-Programmhandbuchs* für einen bestandenen Scan werden erfüllt. • Erneute Scans werden nach Bedarf durchgeführt, um zu bestätigen, dass Schwachstellen gemäß den Anforderungen des *ASV-Programmhandbuchs* für einen bestandenen Scan behoben wurden.	• ASV-Scan-Berichte untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Für die anfängliche PCI DSS-Bewertung gegenüber dieser Anforderung ist es nicht erforderlich, dass vier bestandene Scans innerhalb von 12 Monaten abgeschlossen werden, wenn der Beurteiler Folgendes verifiziert: 1) das letzte Scan-Ergebnis war ein bestandener Scan, 2) die Entität hat dokumentierte Richtlinien und Prozeduren, die einen Scan mindestens alle drei Monate erfordern, und 3) in den Scan-Ergebnissen festgestellte Schwachstellen wurden korrigiert, wie in einem oder mehreren erneuten Scans gezeigt. In den folgenden Jahren nach der ersten PCI DSS-Bewertung müssen jedoch mindestens alle drei Monate bestandene Scans stattgefunden haben. ASV-Scan-Tools können ein breites Spektrum von Netzwerktypen und -topologien scannen. Alle Besonderheiten der Zielumgebung (z. B. Load Balancer, Drittanbieter, ISPs, spezifische Konfigurationen, verwendete Protokolle, Scan-Interferenzen) sollten zwischen dem ASV und dem Scan-Kunden ausgearbeitet werden. Informationen zu den Verantwortlichkeiten des Scan-Kunden, der Scan-Vorbereitung usw. finden Sie im *ASV-Programmhandbuch*, das auf der PCI SSC-Website veröffentlicht ist.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.3.2.1	Externe Schwachstellen-Scans werden nach jeder bedeutenden Änderung wie folgt durchgeführt: • Schwachstellen, die vom CVSS mit 4.0 oder höher bewertet werden, werden behoben. • Erneute Scans werden nach Bedarf ausgeführt. • Scans werden von qualifiziertem Personal durchgeführt und es besteht organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	• Änderungskontrolldokumentation untersuchen. • Personal befragen. • Externe Scans und gegebenenfalls erneute Scan-Berichte untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.4 Externe und interne Penetrationstests werden regelmäßig durchgeführt, und ausnutzbare Schwachstellen und Sicherheitsschwächen werden korrigiert.							
11.4.1	Eine Penetrationstest-Methodik wird von der Entität definiert, dokumentiert und implementiert und umfasst: • In der Branche akzeptierte Penetrationstestansätze. • Abdeckung für den gesamten CDE-Umkreis und die kritischen Systeme. • Tests sowohl innerhalb als auch außerhalb des Netzwerks. • Tests, um Segmentierung und Geltungsbereichs-Reduzierungskontrollen zu validieren. • Penetrationstests auf Anwendungsebene, um mindestens die in Anforderung 6.2.4 aufgeführten Schwachstellen zu identifizieren. • Penetrationstests auf Netzwerkebene, die alle Komponenten umfassen, die Netzwerkfunktionen sowie Betriebssysteme unterstützen. • Überprüfung und Berücksichtigung von Bedrohungen und Schwachstellen, die in den letzten 12 Monaten erfahren wurden. • Dokumentierter Ansatz zur Bewertung und Adressierung des Risikos durch ausnutzbare Schwachstellen und Sicherheitsschwächen, die bei Penetrationstests gefunden werden. • Aufbewahrung der Ergebnisse der Penetrationstests und der Ergebnisse der Behebungsaktivitäten für mindestens 12 Monate. *(fortgesetzt)*	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
	Hinweise zur Anwendbarkeit Das Testen innerhalb des Netzwerks (oder „internes Penetrationstesten“) bedeutet das Testen sowohl innerhalb der CDE als auch in die CDE von vertrauenswürdigen und nicht vertrauenswürdigen internen Netzwerken. Das Testen von außerhalb des Netzwerks (oder „externes“ Penetrationstesten) bedeutet das Testen des exponierten externen Umkreises von vertrauenswürdigen Netzwerken und kritischen Systemen, die mit öffentlichen Netzwerkinfrastrukturen verbunden sind oder darauf zugänglich sind.						
11.4.2	Interne Penetrationstests werden durchgeführt: • Gemäß der definierten Methodik der Entität. • Mindestens einmal alle 12 Monate. • Nach jeder bedeutenden Aktualisierung oder jeder Änderung der Infrastruktur oder Anwendung. • Durch eine qualifizierte interne Ressource oder einen qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	• Geltungsbereich der Arbeit untersuchen. • Ergebnisse vom letzten externen Penetrationstests untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
11.4.3	Externe Penetrationstests werden durchgeführt: • Gemäß der definierten Methodik der Entität. • Mindestens einmal alle 12 Monate. • Nach jeder bedeutenden Aktualisierung oder jeder Änderung der Infrastruktur oder Anwendung. • Durch eine qualifizierte interne Ressource oder einen qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	• Geltungsbereich der Arbeit untersuchen. • Ergebnisse vom letzten externen Penetrationstests untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort* (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.4.4	Ausnutzbare Schwachstellen und Sicherheitsschwächen, die bei Penetrationstests gefunden wurden, werden wie folgt korrigiert: • Entsprechend der Bewertung der Entität bezüglich des Risikos durch das Sicherheitsproblem wie in Anforderung 6.3.1 definiert. • Penetrationstests werden wiederholt, um die Korrekturen zu verifizieren.	• Penetrationstest-Ergebnisse untersuchen.	☐	☐	☐	☐	☐
11.4.5	Wenn Segmentierung verwendet wird, um die CDE von anderen Netzwerken zu isolieren, werden Penetrationstests auf den Segmentierungskontrollen wie folgt durchgeführt: • Mindestens einmal alle 12 Monate und nach jeder Änderung der Segmentierungskontrollen/-methoden • Abdeckung aller verwendeten Segmentierungskontrollen/-methoden. • Gemäß der definierten Penetrationstest-Methodik der Entität. • Bestätigung, dass die Segmentierungskontrollen/-methoden betriebsbereit und effektiv sind und die CDE von allen Systemen außerhalb des Geltungsbereichs isolieren. • Bestätigung der Wirksamkeit jeglicher Verwendung von Isolation, um Systeme mit unterschiedlichen Sicherheitsstufen zu trennen (siehe Anforderung 2.2.3). • Durchgeführt von einer qualifizierten internen Ressource oder einem qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	• Segmentierungskontrollen untersuchen. • Penetrationstest-Methodik überprüfen. • Die Ergebnisse vom letzten Penetrationstests untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.4.6	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter.***						
11.4.7	***Zusätzliche Anforderungen nur für Multi-Mandanten-Dienstleistungsanbieter.***						
11.5 Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und es wird darauf reagiert.							
11.5.1	Eindringungs-Erkennungs- und/oder Eindringungs-Verhinderungs-Techniken werden verwendet, um Eindringungen in das Netzwerk wie folgt zu erkennen und/oder zu verhindern: • Der gesamte Verkehr wird im Umkreis der CDE überwacht. • Der gesamte Verkehr wird an kritischen Stellen in der CDE überwacht. • Das Personal wird vor vermuteten Kompromittierungen gewarnt. • Alle Engines, Baselines und Signaturen für Eindringungs-Erkennung und -Verhinderung werden auf dem neuesten Stand gehalten.	• Systemkonfigurationen und Netzwerkdiagramme untersuchen. • Systemkonfigurationen untersuchen. • Verantwortliches Personal befragen. • Anbieterdokumentation untersuchen.	☐	☐	☐	☐	☐
11.5.1.1	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter.***						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.5.2	Ein Mechanismus zur Erkennung von Änderungen (zum Beispiel Tools zur Überwachung der Dateiintegrität) wird wie folgt eingesetzt: • Um das Personal auf nicht autorisierte Änderungen (einschließlich Änderungen, Ergänzungen und Löschungen) kritischer Dateien aufmerksam zu machen. • Um kritische Dateivergleiche mindestens einmal wöchentlich durchzuführen.	• Systemeinstellungen für den Änderungserfassungsmechanismus untersuchen. • Überwachte Dateien untersuchen. • Ergebnisse der Überwachungsaktivitäten untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Für Zwecke der Änderungserkennung sind kritische Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung jedoch auf eine Systemkompromittierung oder das Risiko einer Kompromittierung hinweisen könnte. Änderungserkennungsmechanismen wie Produkte zur Überwachung der Dateiintegrität werden normalerweise mit kritischen Dateien für das zugehörige Betriebssystem vorkonfiguriert. Andere kritische Dateien, wie für benutzerdefinierte Anwendungen, müssen von der Entität (d.h. dem Händler oder Dienstleistungsanbieter) bewertet und definiert werden.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
11.6 Nicht autorisierte Änderungen auf Zahlungsseiten werden erkannt und es wird darauf reagiert.							
11.6.1	Ein Änderungs- und Manipulationserkennungsmechanismus wird wie folgt eingesetzt:						
	• Um das Personal über nicht autorisierte Änderungen (einschließlich Anzeichen für Kompromittierung, Änderungen, Ergänzungen und Löschungen) an den sicherheitsrelevanten HTTP-Sicherheits-Kopfzeilen und den Skriptinhalten von Zahlungsseiten, wie sie vom Verbraucherbrowser empfangen werden, zu warnen.	• Systemeinstellungen und die Mechanismus-Konfigurationseinstellungen untersuchen. • Überwachte Zahlungsseiten untersuchen. • Ergebnisse der Überwachungsaktivitäten untersuchen.	☐	☐	☐	☐	☐
	• Der Mechanismus ist so konfiguriert, dass er die empfangene HTTP-Kopfzeile und die Zahlungsseite bewertet.	• Die Mechanismus-Konfigurationseinstellungen untersuchen. • Konfigurationseinstellungen untersuchen. • Verantwortliches Personal befragen. • Gegebenenfalls die gezielte Risikoanalyse untersuchen.	☐	☐	☐	☐	☐
	• Die Mechanismusfunktionen werden wie folgt durchgeführt: – Mindestens wöchentlich **ODER** – Regelmäßig (in der Häufigkeit, die in der gezielten Risikoanalyse der Entität definiert ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird. *(fortgesetzt)*		☐	☐	☐	☐	☐

PCI DSS-Anforderung	Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
		Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
Hinweise zur Anwendbarkeit						
Diese Anforderung gilt auch für Entitäten mit einer oder mehreren Webseiten, die eine eingebettete Zahlungsseite/ein eingebettetes Zahlungsformular eines TPSP/Zahlungsabwicklers enthalten (z. B. ein oder mehrere Inline-Frames oder iframes). Diese Anforderung gilt nicht für Entitäten für Skripte in eingebetteten Zahlungsseiten/-formularen eines TPSP/Zahlungsabwicklers (z. B. ein oder mehrere Iframes), wenn die Entität eine Zahlungsseite/ein Zahlungsformular eines TPSP/Zahlungsabwicklers auf ihrer Webseite einbindet. Skripte in eingebetteten Zahlungsseiten/-formularen des TPSP/Zahlungsabwicklers müssen vom TPSP/Zahlungsabwickler entsprechend dieser Anforderung verwaltet werden. Die Absicht dieser Anforderung besteht nicht darin, dass eine Entität Software in den Systemen oder Browsern ihrer Verbraucher installieren muss, sondern dass die Entität Techniken verwendet, die unter Beispielen in der Spalte PCI DSS-Anleitungen (den PCI DSS-Anforderungen und Testprozeduren) beschrieben werden, um unerwartete Skriptaktivitäten zu verhindern und zu erkennen. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

Beibehaltung einer Informationssicherheitspolitik

Anforderung 12: Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.1 Eine umfassende Informationssicherheitsrichtlinie, die den Schutz des Informationsvermögens der Entität regelt und vorgibt, ist bekannt und aktuell.							
12.1.1	Eine gesamte Richtlinie zur Informationssicherheit ist: • Etabliert. • Veröffentlicht. • Gewartet. • Weitergabe an das gesamte relevante Personal sowie an relevante Anbieter und Geschäftspartner.	• Die Informationssicherheitsrichtlinie untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
12.1.2	Die Informationssicherheitsrichtlinie wird: • Mindestens alle 12 Monate überprüft. • Bei Bedarf aktualisiert, um Änderungen der Geschäftszielsetzungen oder Risiken für die Umwelt widerzuspiegeln	• Die Informationssicherheitsrichtlinie untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
12.1.3	Die Sicherheitsrichtlinie definiert die Rollen und Verantwortlichkeiten für die Informationssicherheit für das gesamte Personal eindeutig, und das gesamte Personal ist sind sich seiner Verantwortung für die Informationssicherheit bewusst und erkennt diese an.	• Die Informationssicherheitsrichtlinie untersuchen. • Verantwortliches Personal befragen. • Dokumentierten Nachweis untersuchen.	☐	☐	☐	☐	☐

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.1.4	Die Verantwortung für die Informationssicherheit wird einem Beauftragten für Informationssicherheit oder einem anderen im Bereich Informationssicherheit sachkundigen Mitglied der Geschäftsleitung formell zugewiesen.	• Die Informationssicherheitsrichtlinie untersuchen.	☐	☐	☐	☐	☐
12.2 Richtlinien zur akzeptablen Verwendung für Endbenutzertechnologien werden definiert und implementiert.							
12.2.1	Richtlinien zur akzeptablen Verwendung für Endbenutzertechnologien werden dokumentiert und implementiert, einschließlich: • Ausdrückliche Genehmigung durch autorisierte Parteien. • Akzeptable Verwendungen der Technologie. • Liste der Produkte, die vom Unternehmen für die Verwendung durch Mitarbeiter freigegeben wurden, einschließlich Hardware und Software.	• Akzeptable Verwendungsrichtlinien untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Beispiele für Endbenutzertechnologien, für die akzeptable Verwendungsrichtlinien erwartet werden, beinhalten, sind jedoch nicht darauf beschränkt: Fernzugriff und drahtlose Technologien, Laptops, Tablets, Mobiltelefone und entfernbare elektronische Medien, E-Mail- und Internetverwendung.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.3 Risiken für die Karteninhaberdatenumgebung werden formell identifiziert, bewertet und verwaltet.							
12.3.1	Für jede PCI DSS-Anforderung, Für jede PCI DSS-Anforderung, die den Abschluss einer gezielten Risikoanalyse festlegt, wird die Analyse dokumentiert und umfasst: • Identifizierung der zu schützenden Assets. • Identifizierung der Bedrohung(en), gegen die die Anforderung schützt. • Identifizierung von Faktoren, die zur Wahrscheinlichkeit und/oder Auswirkung beitragen, dass eine Bedrohung realisiert wird. • Ergebnisanalyse, die bestimmt und begründet, wie die Häufigkeit oder die Prozesse, die von der Entität definiert werden, um die Anforderung zu erfüllen, minimiert die Wahrscheinlichkeit und/oder die Auswirkung, dass die Bedrohung realisiert wird. • Überprüfung jeder gezielten Risikoanalyse mindestens alle 12 Monate, um zu bestimmen, ob die Ergebnisse noch gültig sind oder ob eine aktualisierte Risikoanalyse erforderlich ist • Durchführung von aktualisierten Risikoanalysen bei Bedarf, wie von der jährlichen Überprüfung bestimmt ist.	• Dokumentierte Richtlinien und Prozeduren untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
12.3.2	***Diese Anforderung bezieht sich speziell auf den kundenspezifischen Ansatz und gilt nicht für Entitäten, die einen Fragebogen zur Selbstbewertung ausfüllen.***						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.3.3	Die verwendeten kryptografischen Chiffrensammlungen und Protokolle werden mindestens alle 12 Monate dokumentiert und überprüft, einschließlich mindestens der folgenden: • Ein aktuelles Inventar aller verwendeten kryptografischen Chiffrensammlungen und Protokolle, einschließlich Zweck und wo sie verwendet werden. • Aktive Überwachung von Branchentrends in Bezug auf die dauerhafte Funktionsfähigkeit aller verwendeten kryptografischen Chiffrensammlungen und Protokolle. • Dokumentation eines Plans, um auf erwartete Änderungen bei kryptografischen Schwachstellen zu reagieren.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Die Anforderung gilt für alle kryptografischen Ziffersuiten und Protokolle, die zur Erfüllung der PCI DSS-Anforderungen verwendet werden, einschließlich, aber nicht beschränkt auf solche, die verwendet werden, um PAN bei der Speicherung und Übertragung unlesbar zu machen, um Passwörter zu schützen und als Teil der Authentifizierung des Zugriffs. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.3.4	Die verwendeten Hardware- und Softwaretechnologien werden mindestens alle 12 Monate überprüft, einschließlich mindestens der folgenden: • Analyse, dass die Technologien weiterhin umgehend Sicherheitsfehlerbehebungen von Anbietern erhalten. • Analyse, dass die Technologien die PCI DSS-Einhaltung der Entität weiterhin unterstützen (und nicht ausschließen). • Dokumentation aller Branchenankündigungen oder Trends im Zusammenhang mit einer Technologie, wie wenn ein Anbieter Pläne für das „Ende des Lebenszyklus“ einer Technologie angekündigt hat. • Dokumentation eines von der Geschäftsleitung genehmigten Plans zur Behebung veralteter Technologien, einschließlich derer, für die Anbieter Pläne zum „Ende des Lebenszyklus“ angekündigt haben.	• Dokumentation untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
12.4 PCI DSS-Einhaltung wird verwaltet.							
12.4.1	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter.*						
12.4.2	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter.*						
12.4.2.1	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.5 Der PCI DSS-Geltungsbereich wird dokumentiert und validiert.							
12.5.1	Ein Inventar der Systemkomponenten, die für PCI DSS gelten, einschließlich einer Beschreibung der Funktion/Verwendung, wird geführt und auf dem neuesten Stand gehalten.	• Das Inventar untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
12.5.2	Der PCI DSS-Geltungsbereich wird dokumentiert und von der Entität mindestens einmal alle 12 Monate und bei bedeutenden Änderungen an der Umgebung innerhalb des Geltungsbereichs bestätigt.	• Dokumentierte Ergebnisse von Geltungsbereichüberprüfungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Die Scoping-Validierung beinhaltet mindestens:						
	• Identifizieren aller Datenflüsse für die verschiedenen Zahlungsphasen (zum Beispiel Autorisierung, Erfassung der Abrechnung, Rückbuchungen und Rückerstattungen) und Akzeptanzkanäle (zum Beispiel Karte vorhanden, Karte Nicht Vorhanden und E-Commerce).	• Dokumentierte Ergebnisse von Geltungsbereichüberprüfungen untersuchen.	☐	☐	☐	☐	☐
	• Aktualisieren aller Datenflussdiagramme gemäß Anforderung 1.2.4.		☐	☐	☐	☐	☐
	• Identifizieren aller Standorte, an denen Kontendaten gespeichert, verarbeitet und übermittelt werden, einschließlich, aber nicht beschränkt auf: 1) alle Standorte außerhalb der derzeit definierten CDE, 2) Anwendungen, die CHD verarbeiten, 3) Übertragungen zwischen Systemen und Netzwerken, und 4) Datei-Backups.		☐	☐	☐	☐	☐
	• Identifizierung aller Systemkomponenten in der CDE, die mit der CDE verbunden sind oder die die Sicherheit der CDE beeinträchtigen könnten. *(fortgesetzt)*		☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
	• Identifizierung aller verwendeten Segmentierungskontrollen und der Umgebung(en), aus denen die CDE segmentiert wird, einschließlich der Begründung für Umgebungen, die außerhalb des Geltungsbereichs liegen.		☐	☐	☐	☐	☐
	• Identifizieren aller Verbindungen von dritten Entitäten mit Zugriff auf die CDE.		☐	☐	☐	☐	☐
	• Bestätigung, dass alle identifizierten Datenflüsse, Kontodaten, Systemkomponenten, Segmentierungskontrollen und Verbindungen von Dritten mit Zugriff auf die CDE im Geltungsbereich enthalten sind.		☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Diese jährliche Bestätigung des PCI DSS-Geltungsbereichs ist eine Aktivität, die voraussichtlich von der zu bewertenden Entität durchgeführt wird, und ist nicht identisch mit der Scoping-Bestätigung, die vom Bewerter der Entität während der jährlichen Bewertung durchgeführt wird, noch soll sie durch diese ersetzt werden						
12.5.2.1	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter.***						
12.5.3	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter.***						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.6 Die Aufklärung über das Sicherheitsbewusstsein ist eine fortlaufende Aktivität.							
12.6.1	Ein formales Sicherheitsbewusstseinsprogramm wird implementiert, um das gesamte Personal auf die Informationssicherheitsrichtlinien und -prozeduren der Entität und seine Rolle beim Schutz der Karteninhaberdaten aufmerksam zu machen.	• Das Sicherheitsbewusstseinsprogramm untersuchen.	☐	☐	☐	☐	☐
12.6.2	Das Sicherheitsbewusstseinsprogramm wird: • Mindestens einmal alle 12 Monate überprüft und • Nach Bedarf aktualisiert, um neue Bedrohungen und Schwachstellen zu adressieren, die sich auf die Sicherheit der Karteninhaberdaten und/oder sensiblen Authnetifizierungsdaten der Entität oder auf die dem Personal bereitgestellten Informationen über ihre Rolle beim Schutz von Karteninhaberdaten auswirken können.	• Sicherheitsbewusstseinsprogrammінhalt untersuchen. • Nachweise von Überprüfungen untersuchen. • Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
12.6.3	Das Personal erhält folgende Sicherheitsbewusstseinsschulungen: • Bei Einstellung und mindestens einmal alle 12 Monate. • Es werden mehrere Kommunikationsmethoden verwendet. • Das Personal bestätigt mindestens einmal alle 12 Monate, dass es die Informationssicherheitsrichtlinie und -prozeduren gelesen und verstanden hat.	• Sicherheitsbewusstseinsprogrammaufzeichnungen untersuchen. • Zuständiges Personal befragen. • Die Sicherheitsbewusstseinsprogramm-Materialien untersuchen. • Personalbestätigungen untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.6.3.1	Die Sicherheitsbewusstseinsschulung umfasst das Bewusstsein für Bedrohungen und Schwachstellen, die sich auf die Sicherheit der Karteninhaberdaten und/oder sensiblen Authnetifizierungsdaten auswirken könnten, einschließlich, aber nicht beschränkt auf: • Phishing und verwandte Angriffe. • Social Engineering.	• Sicherheitsbewusstseinsprogrammschulungsinhalt untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Siehe Anforderung 5.4.1 in PCI DSS für Anleitungen zum Unterschied zwischen technischen und automatisierten Kontrollen, um Phishing-Angriffe zu erkennen und Benutzer vor ihnen zu schützen, und diese Anforderung für die Bereitstellung von Sicherheitsbewusstseins-Schulungen der Benutzer betreffs Phishing und Social Engineering. Dies sind zwei getrennte und unterschiedliche Anforderungen, und eine wird nicht erfüllt, indem Kontrollen implementiert werden, die von der anderen gefordert werden. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
12.6.3.2	Die Sicherheitsbewusstseinsschulung umfasst das Bewusstsein für die akzeptable Verwendung von Endbenutzertechnologien gemäß Anforderung 12.2.1.	• Sicherheitsbewusstseinsprogrammschulungsinhalt untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.7 Das Personal wird überprüft, um Risiken durch Insider-Bedrohungen zu reduzieren.							
12.7.1	Potentielles Personal, das Zugriff auf die CDE haben wird, wird vor der Einstellung im Rahmen der örtlichen Gesetze überprüft, um das Risiko von Angriffen aus internen Quellen zu minimieren.	• Verantwortliches Personal der Personalabteilung befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Für potenzielles Personal, das für Positionen wie Ladenkassierer eingestellt werden soll, die beim Ermöglichen einer Transaktion nur Zugriff auf jeweils eine Kartennummer haben, ist diese Anforderung nur eine Empfehlung.						
12.8 Das Risiko für Informationsassets im Zusammenhang mit den Beziehungen zu dritten Dienstleistungsanbietern (TPSP) wird verwaltet.							
12.8.1	Eine Liste aller dritten Dienstleistungsanbieter, (TPSPs), mit denen Kontodaten geteilt werden oder die die Sicherheit von Kontodaten beeinträchtigen könnten, wird geführt, einschließlich einer Beschreibung für jeden der bereitgestellten Dienstleistungen.	• Richtlinien und Prozeduren untersuchen. • Liste von TPSPs untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit						
	Die Verwendung eines PCI DSS-konformen TPSP macht eine Entität nicht PCI DSS-konform und enthebt sie auch nicht der Verantwortung für ihre eigene PCI DSS-Einhaltung.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.8.2	Schriftliche Vereinbarungen mit TPSPs werden wie folgt gewartet: • Mit allen TPSPs, mit denen Kontodaten geteilt werden oder die die Sicherheit der CDE beeinträchtigen könnten, werden schriftliche Vereinbarungen aufrechterhalten. • Schriftliche Vereinbarungen beinhalten Bestätigungen von TPSPs, dass TPSPs für die Sicherheit von Kontodaten verantwortlich sind, die die TPSPs besitzen oder anderweitig im Namen der Entität speichern, verarbeiten oder übertragen, oder in dem Umfang, dass die TPSPs sich auf die Sicherheit der Karteninhaberdaten und/oder der sensiblen Authentifizierungsdaten der Entität auswirken könnten.	• Richtlinien und Prozeduren untersuchen. • Schriftliche Vereinbarungen mit TPSPs untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Der genaue Wortlaut einer Vereinbarung hängt von den Details der bereitgestellten Dienstleistung und den jeder Partei zugewiesenen Verantwortlichkeiten ab. Die Vereinbarung muss nicht den genauen Wortlaut enthalten, der in dieser Anforderung bereitgestellt ist. Die schriftliche Bestätigung des TPSP ist eine Bestätigung, die besagt, dass der TPSP für die Sicherheit der Kontodaten verantwortlich ist, die er im Namen des Kunden speichert, verarbeitet oder überträgt, oder in dem Maße, in dem der TPSP die Sicherheit der Karteninhaberdaten und/oder sensiblen Authentifizierungsdaten des Kunden beeinflussen kann. Der Nachweis, dass ein TPSP die PCI DSS-Anforderungen erfüllt, ist nicht dasselbe wie eine in dieser Anforderung angegebenen schriftliche Bestätigung. Eine PCI DSS-Einhaltungsbescheinigung (AOC), eine Erklärung auf der Webseite eines Unternehmens, eine Richtlinienerklärung, eine Verantwortungsmatrix oder andere Nachweise, die nicht in einer schriftlichen Vereinbarung enthalten sind, stellen beispielsweise keine schriftliche Bestätigung dar.						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.8.3	Für die Beauftragung von TPSPs wird ein etablierter Prozess implementiert, einschließlich einer ordnungsgemäßen Sorgfaltspflicht vor der Beauftragung.	• Richtlinien und Prozeduren untersuchen. • Nachweis untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.8.4	Es wird ein Programm implementiert, um den PCI DSS-Einhaltungsstatus der TPSPs mindestens einmal alle 12 Monate zu überwachen.	• Richtlinien und Prozeduren untersuchen. • Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Wenn eine Entität eine Vereinbarung mit einem TPSP zur Erfüllung der PCI DSS-Anforderungen im Namen der Entität hat (zum Beispiel über eine Firewall-Dienstleistung), muss die Entität mit dem TPSP zusammenarbeiten, um sicherzustellen, dass die anwendbaren PCI DSS-Anforderungen erfüllt werden. Wenn der TPSP die geltenden PCI DSS-Anforderungen nicht erfüllt, dann sind diese Anforderungen für das Unternehmen auch "Nicht Vorhanden".						
12.8.5	Es werden Informationen darüber verwaltet, welche PCI DSS-Anforderungen von jedem TPSP verwaltet werden, welche von der Entität verwaltet werden und welche zwischen dem TPSP und der Entität geteilt werden.	• Richtlinien und Prozeduren untersuchen. • Dokumentation untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐
12.9 Dritte Dienstleistungsanbieter (TPSPs) unterstützen die PCI DSS-Einhaltung ihrer Kunden.							
12.9.1	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter.***						
12.9.2	***Zusätzliche Anforderungen nur für Dienstleistungsanbieter.***						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.10 Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf die CDE auswirken könnten, wird umgehend reagiert.							
12.10.1	Ein Vorfallantwortplan ist vorhanden und kann im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls aktiviert werden. Der Plan umfasst, ist aber nicht beschränkt, Folgendes: • Rollen, Verantwortlichkeiten, und Kommunikations- und Kontaktstrategien im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls, mindestens einschließlich der Benachrichtigung von Zahlungsmarken und Erwerbern. • Vorfallantwortprozeduren mit spezifischen Eindämmungs- und Minderungsaktivitäten für verschiedene Arten von Vorfällen. • Prozeduren zur Wiederherstellung und Kontinuität des Geschäftsbetriebs. • Daten-Backup-Prozesse. • Analyse der gesetzlichen Anforderungen zur Meldung von Kompromittierungen. • Abdeckungen und Antworten aller kritischen Systemkomponenten. • Referenz auf oder Einschluss von Vorfallantwortprozeduren von den Zahlungsmarken.	• Den Vorfallantwortplan untersuchen. • Personal befragen. • Dokumentation von zuvor gemeldeten Vorfällen untersuchen.	☐	☐	☐	☐	☐
12.10.2	Mindestens einmal alle 12 Monate wird der Reaktionsplan für Sicherheitsvorfälle: • Überprüft und der Inhalt wird bei Bedarf aktualisiert. • Getestet, einschließlich aller in Anforderung 12.10.1 aufgeführten Elemente.	• Personal befragen. • Dokumentation untersuchen.	☐	☐	☐	☐	☐
12.10.3	Spezifisches Personal steht rund um die Uhr zur Verfügung, um auf vermutete oder bestätigte Sicherheitsvorfälle zu reagieren.	• Verantwortliches Personal befragen. • Dokumentation untersuchen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.10.4	Das Personal, das für die Antwort auf vermutete und bestätigte Sicherheitsvorfälle verantwortlich ist, wird angemessen und regelmäßig in ihren Verantwortlichkeiten für Vorfallsantwort geschult.	• Personal für die Reaktion auf Vorfälle befragen. • Schulungsdokumentation untersuchen.	☐	☐	☐	☐	☐
12.10.4.1	Die Häufigkeit der regelmäßigen Schulungen für das Personal zur Vorfallsantwort ist in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3,1 angegebenen Elementen durchgeführt wird.	• Die gezielte Risikoanalyse untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ (Eine Antwort für jede Anforderung ankreuzen)				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.10.5	Der Sicherheits-Vorfallantwortsplan umfasst die Überwachung und Antwort auf Warnungen von Sicherheitsüberwachungssystemen, einschließlich, aber nicht beschränkt auf: • Eindringungs-Erkennungs- und Eindringungs-Verhinderungs-Systeme. • Netzwerksicherheitskontrollen • Änderungserkennungsmechanismen für kritische Dateien. • Den Änderungs- und Manipulationserkennungsmechanismus für Zahlungsseiten. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Erkennung von *nicht autorisierten* drahtlosen Zugriffspunkte.	• Dokumentation untersuchen. • Prozesse zur Reaktion auf Vorfälle beachten.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Der obige Aufzählungspunkt (für die Überwachung und Antwort auf Warnungen von einem Änderungs- und Manipulationserkennungsmechanismus für Zahlungsseiten) ist eine bewährte Praktik bis zum 31. März 2025, danach ist er als Teil von Anforderung 12.10.5 erforderlich und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						
12.10.6	Der Sicherheits-Vorfallantwortsplan wird gemäß den gewonnenen Erkenntnissen und zur Einbeziehung von Branchenentwicklungen geändert und weiterentwickelt.	• Richtlinien und Prozeduren untersuchen. • Den Sicherheits-Vorfallreaktionsplan untersuchen. • Verantwortliches Personal befragen.	☐	☐	☐	☐	☐

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
12.10.7	Es sind Vorfallantwortsprozeduren vorhanden, die beim Nachweis von gespeicherter PAN an einem Ort eingeleitet werden, an dem dies nicht zu erwarten ist, und umfassen: • Bestimmen, was zu tun ist, wenn PAN außerhalb der CDE entdeckt wird, einschließlich ihres Abrufs, sicheren Löschens und/oder Migration in die aktuell definierte CDE, soweit zutreffend. • Identifizieren, ob sensible Authentifizierungsdaten mit PAN gespeichert sind. • Bestimmen, woher die Kontodaten stammten und wie sie dort gelandet sind, wo es nicht erwartet wurde. • Beheben von Datenlecks oder Prozesslücken, die dazu führten, dass die Kontodaten dort waren, wo es nicht erwartet wurde.	• Dokumentierte Prozesse zur Reaktion auf Vorfälle untersuchen. • Personal befragen. • Aufzeichnungen über Reaktionsaktionen untersuchen.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*						

Anhang A: Zusätzliche PCI DSS-Anforderungen

Anhang A1: Zusätzliche PCI DSS-Anforderungen für Multi-Mandanten-Dienstleistungsanbieter

Dieser Anhang wird nicht für Händlerbewertungen verwendet.

Anhang A2: Zusätzliche PCI DSS-Anforderungen für Entitäten, die SSL/Early TLS für Karte anwesend POS-POI-Terminalverbindungen verwenden

PCI DSS-Anforderung		Erwartetes Testen	Antwort♦ *(Eine Antwort für jede Anforderung ankreuzen)*				
			Vorhanden	Vorhanden mit CCW	Nicht Anwendbar	Nicht Getestet	Nicht Vorhanden
A2.1 POI-Terminals, die SSL und/oder frühe Versionen von TLS verwenden, sind für bekannte SSL/TLS-Ausnutzungen nicht anfällig.							
A2.1.1	Wenn POS-POI-Terminals am Händler- oder Zahlungsakzeptanzstandort SSL und/oder frühes TLS verwenden, bestätigt die Entität, dass die Geräte für bekannte Ausnutzung für diese Protokolle nicht anfällig sind.	• Dokumentation (zum Beispiel Anbieterdokumentation, System-/Netzwerkkonfigurationsdetails) untersuchen, die verifiziert, dass die Geräte gegenüber bekannten Ausnutzungen für SSL/frühes TLS nicht anfällig sind.	☐	☐	☐	☐	☐
	Hinweise zur Anwendbarkeit Diese Anforderung soll für die Entität mit dem POS-POI-Terminal gelten, wie einen Händler. Diese Anforderung gilt nicht für Dienstleistungsanbieter, die als Terminierungs- oder Verbindungspunkt zu diesen POS-POI-Terminals dienen. Die Anforderungen A2.1.2 und A2.1.3 gelten für POS-POI-Dienstleistungsanbieter. Die Zulassung von POS-POI-Terminals, die derzeit nicht gegenüber Ausnutzungen anfällig sind, basiert auf den derzeit bekannten Risiken. Wenn neue Ausnutzungen eingeführt werden, für die POS-POI-Terminals anfällig sind, müssen die POS-POI-Terminals sofort aktualisiert werden.						
A2.1.2	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter.*						
A2.1.3	*Zusätzliche Anforderungen nur für Dienstleistungsanbieter.*						

♦ *Informationen zu diesen Anwortmöglichkeiten siehe im Abschnitt „Anforderungsantworten“ (Seite vi).*

Anhang A3: Ergänzende Validierung für designierte Entitäten (DESV)

Dieser Anhang gilt nur für Entitäten, die von Zahlungsmarke(n) oder Erwerbern als Erfordern einer zusätzlichen Validierung bestehender PCI-DSS-Anforderungen bezeichnet werden. Entitäten, die diesen Anhang validieren müssen, sollten die DESV-Vorlage für ergänzende Berichte und die ergänzende Konformitätsbescheinigung für die Berichterstattung verwenden und sich mit der jeweiligen Zahlungsmarke und/oder dem Erwerber bezüglich der Einreichungsverfahren beraten.

Anhang B: Arbeitsblatt Kompensationssteuerungen

Dieser Anhang muss ausgefüllt werden, um kompensierende Kontrollen für irgendwelche Anforderungen zu definieren, bei denen Vorhanden mit CCW ausgewählt wurde.

Hinweis: *Nur Entitäten, die eine legitime und dokumentierte technologische oder geschäftliche Einschränkung haben, können die Verwendung von kompensierenden Kontrollen in Betracht ziehen, um die Einhaltung zu erreichen.*

Informationen zu Kompensationskontrollen und Anleitungen zum Ausfüllen dieses Arbeitsblatts finden Sie in den Anhängen B und C des PCI DSS.

Anforderungsnummer und -definition:

	Erforderte Informationen	Erklärung
1. Einschränkungen	Die legitimen technischen oder geschäftlichen Einschränkungen dokumentieren, die die Einhaltung der ursprünglichen Anforderung verhindern.	
2. Definition von kompensierenden Kontrollen	Die kompensierenden Kontrollen definieren: erklären, wie sie die Ziele der ursprünglichen Kontrolle und das erhöhte Risiko, falls vorhanden, adressieren.	
3. Zielsetzung	Die Zielsetzung der ursprünglichen Kontrolle definieren.	
	Die Zielsetzung identifizieren, die durch die kompensierende Kontrolle erreicht wird. ***Hinweis:*** *Dies kann, muss aber nicht, die angegebene Zielsetzung des kundenspezifischen Ansatzes sein, die für diese Anforderung im PCI DSS aufgeführt ist.*	
4. Identifiziertes Risiko	Jedes zusätzliche Risiko identifizieren, das durch das Fehlen der ursprünglichen Kontrolle entsteht.	
5. Validierung von kompensierenden Kontrollen	Definieren, wie die kompensierenden Kontrollen validiert und getestet wurden.	
6. Aufrechterhaltung	Prozess(e) und Kontrollen definieren, um kompensierende Kontrollen aufrechtzuerhalten.	

Anhang C: Erklärung der als Nicht Anwendbar vermerkten Anforderungen

Dieser Anhang muss für jede Anforderung ausgefüllt werden, bei der Nicht anwendbar ausgewählt wurde.

Anforderung	Grund der Anforderung ist Nicht Anwendbar
Beispiel:	
Anforderung 3.5.1	*Kontodaten werden nie elektronisch gespeichert*

Anhang D: Erklärung der als Nicht Getestet vermerkten Anforderungen

Dieser Anhang muss für jede Anforderung ausgefüllt werden, bei der Nicht Getestet ausgewählt wurde.

Anforderung	Beschreibung der Anforderung(en) Nicht Getestet	Beschreiben, warum die Anforderung(en) von der Bewertung ausgeschlossen wurde(n)
Beispiele:		
Anforderung 10	*Keine Anforderungen von Anforderung 10 wurden getestet.*	*Diese Bewertung deckt nur Anforderungen in Meilenstein 1 des priorisierten Ansatzes ab.*
Anforderungen 1-8, 10-12	*Für diese Bewertung wurde nur Anforderung 9 überprüft. Alle anderen Anforderungen wurden ausgeschlossen.*	*Das Unternehmen ist ein physischer Hosting-Anbieter (CO-LO), und für diese Bewertung wurden nur physische Sicherheitskontrollen berücksichtigt.*

Abschnitt 3: Validierungs- und Bescheinigungsdetails

Teil 3. PCI DSS-Validierung

Diese AOC basiert auf Ergebnissen, die in SAQ D (Abschnitt 2) mit dem Datum (Datum des Abschlusses der Selbstbewertung) vermerkt sind *TT-MM-JJJJ).*

Unten angeben, ob eine vollständige oder teilweise PCI DSS-Bewertung abgeschlossen wurde:

☐ **Vollständig** – Alle Anforderungen wurden bewertet, daher wurden keine Anforderungen im AOC als Nicht Getestet vermerkt.

☐ **Teilweise** – Eine oder mehrere Anforderungen wurden nicht bewertet und wurden daher im SAQ als Nicht Getestet vermerkt. Jede nicht bewertete Anforderung wird in Teil 2g oben als Nicht Getestet vermerkt.

Basierend auf den im oben erwähnten SAQ D dokumentierten Ergebnissen bestätigt jeder Unterzeichner, der in einem der Teile 3b-3d identifiziert wurde, den folgenden Konformitäts-Status für den in Teil 2 dieses Dokuments identifizierten Händler.

Eins auswählen:

☐	**Konform:** Alle Abschnitte des PCI DSS-SAQ sind vollständig, und alle bewerteten Anforderungen sind entweder als 1) Vorhanden, 2) Vorhanden mit CCW oder 3) Nicht Anwendbar gekennzeichnet, was eine Gesamtbewertung von **KONFORM** ergibt; dabei hat *(Unternehmensname des Händlers)* die Konformität aller PCI DSS-Anforderungen demonstriert, die in diesem SAQ eingeschlossen sind, mit Ausnahme derjenigen, die oben als Nicht Getestet gekennzeichnet sind.
☐	**Nicht konform:** Nicht alle Abschnitte des PCI DSS-SAQ sind vollständig, oder eine oder mehrere Anforderungen sind als „Nicht Vorhanden“ gekennzeichnet, was zu einer Gesamtbewertung **NICHT KONFORM** führt, dadurch hat *(Unternehmensname des Händlers)* die Konformität der PCI DSS-Anforderungen demonstriert, die in diesem SAQ enthalten sind. **Zieldatum** für Konformität: *TT-MM-JJJJ* Ein Händler, der dieses Formular mit einem Status „Nicht konform“ einreicht, muss möglicherweise den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. Bestätigen mit der Entität, an die diese AOC übermittelt wird, *bevor Ausfüllen von Teil 4*.
☐	**Konform, aber mit gesetzlicher Ausnahme:** Eine oder mehrere bewertete Anforderungen im ROC werden aufgrund einer gesetzlichen Einschränkung, die die Erfüllung der Anforderung verhindert, als Nicht Vorhanden gekennzeichnet, und alle anderen bewerteten Anforderungen werden entweder als 1) Vorhanden, 2) Vorhanden mit CCW oder 3) Nicht Anwendbar gekennzeichnet, was zu eine Gesamtbewertung von **KONFORM, ABER MIT RECHTLICHER AUSNAHME** ergibt; dabei hat *(Unternehmensname des Händlers)* die Konformität aller PCI DSS-Anforderungen demonstriert, mit Ausnahme derjenigen, die oben als Nicht Getestet oder aufgrund einer gesetzlichen Einschränkung als Nicht Vorhanden gekennzeichnet sind. Diese Option erfordert eine zusätzliche Überprüfung von der Entität, an die diese AOC übermittelt wird. *Falls ausgewählt, Vervollständigen von Folgendem:*

Betroffene Anforderung	Details wie legale Einschränkungen verhindern, dass die Anforderung erfüllt wird

Teil 3a. Händlerbestätigung

Der/die Unterzeichner bestätigt/bestätigen:

(Alle zutreffenden auswählen)

☐	Der PCI DSS Fragebogen D zur Selbstbewertung, Version 4.0.1 wurde gemäß den darin enthaltenen Anweisungen ausgefüllt.
☐	Alle Informationen in dem oben genannten SAQ und in dieser Bescheinigung geben die Ergebnisse der Bewertung des Händlers in allen wesentlichen Aspekten angemessen wieder.
☐	PCI DSS-Kontrollen werden jederzeit aufrechterhalten, soweit dies für die Umgebung des Händlers gilt.

Teil 3b. Händlerbescheinigung

Unterschrift des geschäftsführenden Händlers ↑	*Datum: TT-MM-JJJJ*
Name des geschäftsführenden Händlers:	*Titel:*

Teil 3c. Qualifizierter Sicherheitsbewerter (QSA)-Bestätigung

Wenn ein QSA an dieser Bewertung beteiligt war oder bei dieser Bewertung half, angeben der durchgeführten Rolle:	☐ QSA führte Testprozeduren durch.
	☐ QSA stellte weitere Hilfe bereit. Falls ausgewählt, beschreiben aller ausgeübten Rollen:

Unterschrift des Haupt-QSA ↑	*Datum: TT-MM-JJJJ*
Name des Haupt-QSA:	

Unterschrift des ordnungsgemäß autorisierten Beauftragten des QSA-Unternehmens ↑	*Datum: TT-MM-JJJJ*
Name des ordnungsgemäß autorisierten Beauftragten:	*QSA-Unternehmen:*

Teil 3d. PCI SSC-Interne Sicherheitsbewerter (ISA)-Beteiligung

Wenn ein oder mehrere ISA(s) an dieser Bewertung beteiligt waren oder sie dabei halfen, angeben der durchgeführten Rolle:	☐ ISA(s) führte(n) Testprozeduren durch.
	☐ ISA(s) stellte(n) weitere Hilfe bereit.. Falls ausgewählt, beschreiben aller ausgeübten Rollen:

Teil 4. Aktionsplan für nicht konforme Anforderungen

Füllen Sie Teil 4 nur auf Anfrage der Entität aus, an die dieses AOC übermittelt wird, und nur, wenn die Bewertung einen nicht konformen Status aufweist, der in Abschnitt 3 aufgelistet ist.

Wenn Sie aufgefordert werden, diesen Abschnitt auszufüllen, wählen Sie die entsprechende Antwort für „Mit den PCI DSS-Anforderungen konform“ für jede Anforderung unten aus. Angeben bei allen „Nein"-Antworten des Datums, an dem der Händler mit der Anforderung voraussichtlich konform sein wird, und eine kurze Beschreibung der Aktionen, die zur Erfüllung der Anforderung ergriffen wurden.

PCI DSS-Anforderung	Beschreibung der Anforderung	Mit den PCI DSS-Anforderungen konform (Eins auswählen)		Behebungsdatum und Aktionen (Wenn „NEIN“ für irgendeine Anforderung ausgewählt wird)
		JA	NEIN	
1	Installation und Wartung von Netzwerksicherheitskontrollen	☐	☐	
2	Anwendung sicherer Konfigurationen auf alle Systemkomponenten	☐	☐	
3	Schutz von gespeicherten Kontodaten	☐	☐	
4	Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke	☐	☐	
5	Schutz aller Systeme und Netzwerke vor bösartiger Software	☐	☐	
6	Entwicklung und Wartung sicherer Systeme und Software	☐	☐	
7	Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach geschäftlichem Bedarf	☐	☐	
8	Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten	☐	☐	
9	Beschränkung des physischen Zugriffs auf Karteninhaberdaten.	☐	☐	
10	Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten	☐	☐	
11	Regelmäßiges Testen der Sicherheit von Systemen und Netzen	☐	☐	
12	Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme	☐	☐	
Anhang A2	Zusätzliche PCI DSS-Anforderungen für Entitäten, die SSL/Early TLS für Karte anwesend POS-POI-Terminalverbindungen verwenden	☐	☐	

Hinweis: *Das PCI Security Standards Council ist ein internationales Normungsgremium, das in Zusammenarbeit mit unserer Stakeholder-Gemeinschaft Ressourcen für Fachleute im Bereich Zahlungssicherheit entwickelt. Die von uns angebotenen Materialien werden in zahlreichen Compliance-Programmen weltweit akzeptiert. Sie sollten sich bei Ihrer jeweiligen Organisation erkundigen, ob dieses Formular in ihrem Programm akzeptiert wird. Nähere Informationen über PCI SSC und unsere Stakeholder-Gemeinschaft finden Sie hier:* *https://www.pcisecuritystandards.org/about_us/.*