Payment Card Industry (PCI)
Datensicherheitsstandard

Selbstbeurteilungsfragebogen D
und Konformitätsbescheinigung

Sonstige SBF-qualifizierte Händler und Dienstanbieter

Version 2.0

Oktober 2010

Dokumentänderungen

Datum	Version	Beschreibung
1. Oktober 2008	1.2	Anpassung der Inhalte an den neuen PCI-DSS v1.2 und Implementieren kleinerer Änderungen in der Ursprungsversion v1.1.
28. Oktober 2010	2.0	Anpassung der Inhalte an die neuen PCI-DSS v2.0 Anforderungen und Prüfverfahren.

Inhalt

PCI-Datensicherheitsstandard: Zugehörige Dokumente

Die folgenden Dokumente wurden als Unterstützung für Händler und Dienstanbieter entwickelt, um sie besser über den PCI-Datensicherheitsstandard (PCI-DSS) und den PCI-DSS SBF zu informieren.

Dokument	Publikum
PCI-Datensicherheitsstandard: Anforderungen und Sicherheitsbeurteilungsverfahren	Alle Händler und Dienstanbieter
PCI-DSS-Navigation: Verständnis des Zwecks der Anforderungen	Alle Händler und Dienstanbieter
PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung	Alle Händler und Dienstanbieter
PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen A und Bescheinigung	Qualifizierte Händler[1]
PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen B und Bescheinigung	Qualifizierte Händler[1]
PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen C-VT und Bescheinigung	Qualifizierte Händler[1]
PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen C und Bescheinigung	Qualifizierte Händler[1]
PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen D und Bescheinigung	Qualifizierte Händler und Dienstanbieter[1]
PCI-Datensicherheitsstandard und Datensicherheitsstandard für Zahlungsanwendungen: Glossar für Begriffe, Abkürzungen und Akronyme	Alle Händler und Dienstanbieter

[1] Informationen zur Bestimmung des angemessenen Selbstbeurteilungsfragebogen finden Sie unter *PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung*, „Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind."

Vorbereitung

Ausfüllen des Selbstbeurteilungsfragebogens

SBF D wurde für alle SBF-qualifizierten Dienstanbieter und Händler entwickelt, die den Beschreibungen der SBF Typ A bis C, wie in der nachstehenden Tabelle kurz und in *Anleitung und Richtlinien zum PCI-DSS Selbstbeurteilungsfragebogen* ausführlich erläutert, nicht entsprechen.

SBF	Beschreibung
A	Händler, bei denen die Karte nicht vorliegt (E-Commerce oder Versandhandel), alle Karteninhaberdaten-Funktionen wurden extern vergeben. *Dies gilt nicht für Händler mit physischer Präsenz.*
B	Händler, die ausschließlich Abdruckgeräte ohne elektronischen Karteninhaberdaten-Speicher verwenden, oder Händler mit eigenständigen Terminals mit Dial-Out-Funktion ohne elektronischen Karteninhaberdaten-Speicher.
C-VT	Händler ausschließlich mit webbasierten virtuellen Terminals ohne elektronischen Karteninhaberdaten-Speicher
C	Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind, kein elektronischer Karteninhaberdaten-Speicher
D	Alle anderen Händler (nicht in den Beschreibungen für SBF A bis C oben enthalten) und **alle Dienstanbieter**, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden.

SBF D gilt für SBF-qualifizierte Händler, die nicht die Kriterien für die SBF A bis C oben erfüllen, sowie alle Dienstanbieter, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden. SBF D Dienstanbieter und Händler müssen die Einhaltung der Anforderungen bestätigen, indem sie den SBF D und die zugehörige Konformitätsbescheinigung ausfüllen.
Während viele Unternehmen, die den SBF D ausfüllen, die Einhaltung aller PCI-DSS-Anforderungen bestätigen müssen, werden einige Unternehmen mit sehr spezifischen Geschäftsmodellen evtl. feststellen, dass einige Anforderungen für sie nicht gelten. Ein Unternehmen, das z. B. überhaupt keine drahtlose Technologie verwendet, muss die Einhaltung der Abschnitte des PCI-DSS, die sich speziell auf die Verwaltung drahtloser Technologien beziehen, nicht validieren. In der nachstehenden Anleitung finden Sie Informationen über den Ausschluss drahtloser Technologie und bestimmte andere spezifische Anforderungen.

Jeder Abschnitt dieses Fragebogens konzentriert sich auf einen bestimmten Sicherheitsbereich und basiert auf den Anforderungen im PCI-DSS.

PCI-DSS-Konformität – Schritte zum Ausfüllen

1. Bewerten Sie Ihre Umgebung auf die Einhaltung des PCI-DSS.
2. Füllen Sie den Selbstbeurteilungsfragebogen (SBF D) gemäß der *Anleitung und den Richtlinien zum Selbstbeurteilungsfragebogen aus.*
3. Führen Sie einen Anfälligkeitsscan mit einem von PCI-SSC zugelassenen Scanninganbieter (Approved Scanning Vendor oder ASV) durch und lassen Sie sich einen bestandenen Scan vom ASV nachweisen.
4. Füllen Sie die Konformitätsbescheinigung vollständig aus.
5. Reichen Sie den SBF, den Nachweis eines bestandenen Scans und die Konformitätsbescheinigung zusammen mit allen anderen erforderlichen Dokumenten bei Ihrem

Acquirer (Händler) oder bei der Zahlungsmarke oder einer anderen Anforderungsstelle (Dienstanbieter) ein.

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

Ausschlusskriterien: Wenn Sie den SBF D ausfüllen müssen, um Ihre PCI-DSS-Konformität zu bestätigen, können folgende Ausnahmen berücksichtigt werden: Lesen Sie unten den Abschnitt „Nichtanwendbarkeit“, um die jeweils zutreffende SBF-Antwort zu erfahren.

- Die für drahtlose Technologie spezifischen Fragen müssen nur beantwortet werden, wenn drahtlose Technologie in Ihrem Netzwerk verwendet wird (Anforderungen 1.2.3, 2.1.1 und 4.1.1). Bitte beachten Sie, dass Anforderung 11.1 (Verwendung eines Prozesses zur Erkennung unbefugter WLAN-Zugriffspunkte) auch beantwortet werden muss, wenn Sie in Ihrem Netzwerk keine drahtlose Technologie verwenden, weil der Prozess alle sicherheitsgefährdenden oder unerlaubten Geräte erfasst, die vielleicht ohne Ihr Wissen angeschlossen wurden.
- Die Fragen zu benutzerdefinierten Anwendungen und Codes (Anforderungen 6.3 und 6.5) müssen nur beantwortet werden, wenn Ihr Unternehmen eigene benutzerdefinierte Anwendungen entwickelt.
- Die Fragen zu den Anforderungen 9.1 bis 9.4 müssen nur von Stellen mit „zugangsbeschränkten Bereichen“, wie hier definiert, beantwortet werden. „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Dazu zählen nicht Bereiche, in denen ausschließlich Point-of-Sale-Terminals vorhanden sind, wie zum Beispiel der Kassenbereich in einem Einzelhandel. Hierin eingeschlossen sind jedoch Back-Office-Serverräume in Einzelhandelsgeschäften, in denen Karteninhaberdaten gespeichert werden, sowie Speicherbereiche für große Mengen an Karteninhaberdaten.

Nichtanwendbarkeit: Diese und alle anderen Anforderungen, die nicht für Ihre Umgebung gelten, müssen im SBF in der Spalte „Spezial“ mit „N/A“ gekennzeichnet werden. Dementsprechend müssen Sie das Arbeitsblatt „Erläuterung der Nichtanwendbarkeit“ im Anhang D für jeden einzelnen Eintrag, der „N/A“ lautet, ausfüllen.

Konformitätsbescheinigung, SBF D – Version für Händler

Anleitung zum Einreichen

Der Händler muss diese Konformitätsbescheinigung einreichen, um zu bestätigen, dass er den Konformitätsstatus mit den *Payment Card Industry Datensicherheitsstandard (PCI-DSS) – Anforderungen und Sicherheitsbeurteilungsverfahren erfüllt.* Füllen Sie alle zutreffenden Abschnitte aus und schlagen Sie die Anleitung zum Einreichen unter „PCI-DSS-Konformität – Schritte zum Ausfüllen“ in diesem Dokument nach.

Teil 1. Informationen zum Händler und qualifizierten Sicherheitsprüfer

Teil 1a. Informationen zum Händlerunternehmen

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

Teil 1b. Informationen zum Unternehmen des qualifizierten Sicherheitsprüfers (falls vorhanden)

Name des Unternehmens:	

QSA-Leiter:		Titel:	
Telefonnr.:		E-Mail:	
Geschäftsadresse:		Ort:	

Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 2 Typ des Händlerunternehmens (alle zutreffenden Optionen auswählen):

☐ Einzelhändler ☐ Telekommunikation ☐ Lebensmitteleinzelhandel und Supermärkte

☐ Erdöl/Erdgas ☐ E-Commerce ☐ Versandhandel

☐ Sonstige (bitte angeben):

Liste der Einrichtungen und Standorte, die in der PCI-DSS-Prüfung berücksichtigt wurden:

Teil 2a. Beziehungen

Steht Ihr Unternehmen in Beziehung zu einem oder mehreren Drittdienstanbietern (z. B. Gateways, Webhosting-Unternehmen, Buchungspersonal von Fluggesellschaften, Vertreter von Kundentreueprogrammen usw.)?	☐ Ja ☐ Nein
Steht Ihr Unternehmen mit mehr als einem Acquirer in Kontakt?	☐ Ja ☐ Nein

Teil 2b. Transaktionsverarbeitung

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

Bitte geben Sie folgenden Informationen bezüglich der Zahlungsanwendungen an, die in Ihrem Unternehmen verwendet werden:

Verwendete Zahlungsanwendung	**Versionsnummer**	**Letzte Validierung gemäß PABP/PA-DSS**

Teil 3. PCI-DSS-Validierung

Anhand der Ergebnisse, die im SBF D mit Datum vom *(Ausfülldatum)* notiert wurden, bestätigt *(Name des Händlerunternehmens)* folgenden Konformitätsstatus (eine Option auswählen):

☐ **Konform:** Alle Abschnitte des PCI SBF sind vollständig und alle Fragen wurden mit „Ja“ beantwortet, woraus sich die Gesamtbewertung **KONFORM** ergeben hat, **und** es wurde ein Scan von einem von PCI-SSC zugelassenen Approved Scanning Vendor (ASV) durchgeführt und bestanden, wodurch *(Name des Händlerunternehmens)* volle Konformität mit dem PCI-DSS gezeigt hat.

☐ **Nicht konform:** Nicht alle Abschnitte des PCI-DSS SBF sind vollständig oder einige Fragen wurden mit „Nein“ beantwortet, woraus sich die Gesamtbewertung **NICHT KONFORM** ergeben hat, **oder** es wurde kein Scan von einem von PCI-SSC zugelassenen Approved Scanning Vendor (AVS) durchgeführt und bestanden, wodurch *(Name des Händlerunternehmens)* nicht die volle Konformität mit dem PCI-DSS gezeigt hat.

Zieldatum für Konformität:

Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

Teil 3a. Bestätigung des Status „Konform“

Der Händler bestätigt:

☐	Der PCI-DSS Selbstbeurteilungsfragebogen D, Version *(Version des SBF)*, wurde den enthaltenen Anleitungen gemäß ausgefüllt.
☐	Alle Informationen im oben genannten SBF und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung in allen materiellen Aspekten korrekt dar.
☐	Mein Zahlungsanwendungsanbieter hat mir bestätigt, dass in meinem Zahlungssystem nach der Autorisierung keine empfindlichen Authentifizierungsdaten gespeichert werden.
☐	Ich habe den PCI-DSS gelesen und erkenne an, dass ich jederzeit die vollständige PCI-DSS-Konformität aufrechterhalten muss.
☐	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifendaten (aus einer Spur),[2] CAV2-, CVC2-, CID- oder CVV2-Daten[3] oder PIN-Daten[4] gespeichert wurden.

[2] Im Magnetstreifen verschlüsselte Daten oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Spurdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

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

Teil 3b. Bestätigung durch den Händler

Unterschrift des Beauftragten des Händlers ↑	*Datum ↑*
Name des Beauftragten des Händlers ↑	*Titel ↑*

Vertretenes Händlerunternehmen ↑

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen Konformitätsstatus für jede Anforderung aus. Wenn Sie eine der Anforderungen mit „NEIN“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung voraussichtlich erfüllen wird. Geben Sie außerdem eine kurze Beschreibung der Aktionen an, die unternommen werden, um die Anforderung zu erfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

PCI-DSS-Anforderung	Anforderungsbeschreibung	Konformitätsstatus (eine Option auswählen)		Abhilfedatum und Aktionen (bei Konformitätsstatus „NEIN“)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	☐	☐	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	☐	☐	
3	Schutz gespeicherter Karteninhaberdaten	☐	☐	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	☐	☐	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	☐	☐	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	☐	☐	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	☐	☐	

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

		Konformitätsstatus (eine Option auswählen)		
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	☐	☐	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	☐	☐	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	☐	☐	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	☐	☐	
12	Pflegen einer Informationssicherheitsrichtlinie für das gesamte Personal	☐	☐	

Konformitätsbescheinigung, SBF D – Version für Dienstanbieter

Anleitung zum Einreichen

Der Dienstanbieter muss diese Konformitätsbescheinigung einreichen, um zu bestätigen, dass er den Konformitätsstatus mit den *Payment Card Industry Datensicherheitsstandard (PCI-DSS) – Anforderungen und Sicherheitsbeurteilungsverfahren erfüllt.* Füllen Sie alle zutreffenden Abschnitte aus und schlagen Sie die Anleitung zum Einreichen unter „PCI-DSS-Konformität – Schritte zum Ausfüllen“ in diesem Dokument nach.

Teil 1. Informationen zu Dienstanbietern und qualifizierten Sicherheitsprüfern

Teil 1a. Informationen zum Dienstanbieterunternehmen

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

Teil 1b. Informationen zum Unternehmen des qualifizierten Sicherheitsprüfers (falls vorhanden)

Name des Unternehmens:	

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

Teil 2. Informationen zur PCI-DSS-Bewertung

Teil 2a. Geleistete Services, die in der PCI-DSS-Bewertung (alle zutreffenden Optionen auswählen) BEURTEILT WURDEN:

☐ 3-D Secure-Hosting-Anbieter	☐ Hosting-Anbieter – Hardware	☐ Zahlungsabwicklung – ATM
☐ Kontoführung	☐ Hosting-Anbieter – Web	☐ Zahlungsabwicklung – MOTO
☐ Autorisierung	☐ Ausstellungsdienste	☐ Zahlungsabwicklung – Internet
☐ Back-Office-Services	☐ Treueprogramme	☐ Zahlungsabwicklung – POS
☐ Rechnungsverwaltung	☐ Verwaltete Services	☐ Prepaid Services
☐ Abwicklung und Abrechnung	☐ Händlerservices	☐ Archivmanagement
☐ Datenaufbereitung	☐ Netzbetreiber/Sender	☐ Steuern/Zahlungen an den Staat
☐ Betrugsmanagement und Ausgleichszahlungen	☐ Zahlungs-Gateway/Switch	
☐ Sonstige (bitte angeben):		

Liste der Einrichtungen und Standorte, die in der PCI-DSS-Prüfung berücksichtigt wurden:

Teil 2b. Markieren Sie bitte unten jegliche Services, die vom Dienstanbieter geleistet wurden, jedoch anlässlich der PCI-DSS-Bewertung *NICHT BEURTEILT WURDEN*:

☐ 3-D Secure-Hosting-Anbieter	☐ Hosting-Anbieter – Hardware	☐ Zahlungsabwicklung – ATM
☐ Kontoführung	☐ Hosting-Anbieter – Web	☐ Zahlungsabwicklung – MOTO
☐ Autorisierung	☐ Ausstellungsdienste	☐ Zahlungsabwicklung – Internet
☐ Back-Office-Services	☐ Treueprogramme	☐ Zahlungsabwicklung – POS
☐ Rechnungsverwaltung	☐ Verwaltete Services	☐ Prepaid Services
☐ Abwicklung und Abrechnung	☐ Händlerservices	☐ Archivmanagement
☐ Datenaufbereitung	☐ Netzbetreiber/Sender	☐ Steuern/Zahlungen an den Staat
☐ Betrugsmanagement und Ausgleichszahlungen	☐ Zahlungs-Gateway/Switch	

☐ Sonstiges (bitte angeben):

Teil 2c. Beziehungen

Hat Ihr Unternehmen eine Beziehung mit einem oder mehreren Drittdienstanbietern (z. B. Gateways, Webhosting-Anbieter, Flugreiseagenturen, Anbieter von Kundentreueprogrammen usw.)? ☐ Ja ☐ Nein

Teil 2d. Transaktionsverarbeitung

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

Verwendete Zahlungsanwendung	Versionsnummer	Letzte Validierung gemäß PABP/PA-DSS

Bitte geben Sie folgenden Informationen bezüglich der Zahlungsanwendungen an, die in Ihrem Unternehmen verwendet werden:

Teil 3. PCI-DSS-Validierung

Anhand der Ergebnisse, die in SBF D mit Datum vom *(Ausfülldatum des SBF)* notiert wurden, bestätigt *(Name des Dienstanbieterunternehmens)* folgenden Konformitätsstatus (eine Option auswählen):

☐ **Konform:** Alle Abschnitte des PCI-SBF sind vollständig und alle Fragen wurden mit „Ja“ beantwortet, woraus sich die Gesamtbewertung **KONFORM** ergeben hat, **und** es wurde ein Scan von einem von PCI-SSC zugelassenen Approved Scanning Vendor (ASV) durchgeführt und bestanden, wodurch *(Name des*

Dienstanbieterunternehmens) volle Konformität mit dem PCI-DSS gezeigt hat.

☐ **Nicht konform:** Nicht alle Abschnitte des PCI-SBF sind vollständig oder einige Fragen wurden mit „Nein“ beantwortet, woraus sich die Gesamtbewertung **NICHT KONFORM** ergeben hat, **oder** es wurde kein Scan von einem von PCI SSC zugelassenen Approved Scanning Vendor (ASV) durchgeführt und bestanden, wodurch *(Name des Dienstanbieterunternehmens)* nicht die volle Konformität mit dem PCI-DSS gezeigt hat.

Zieldatum für Konformität:

Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern*.

Teil 3a. Bestätigung des Status „Konform“

Der Dienstanbieter bestätigt:

☐	Der Selbstbeurteilungsfragebogen D, Version *(Versionsnummer einfügen)*, wurde den enthaltenen Anleitungen gemäß ausgefüllt.
☐	Alle Informationen im oben genannten SBF und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung korrekt dar.
☐	Ich habe den PCI-DSS gelesen und erkenne an, dass ich jederzeit die vollständige PCI-DSS-Konformität aufrechterhalten muss.
☐	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifendaten (aus einer Spur),[5] CAV2-, CVC2-, CID- oder CVV2-Daten[6] oder PIN-Daten[7] gespeichert wurden.

Teil 3b. Bestätigung durch den Dienstanbieter

Unterschrift des Beauftragten des Dienstanbieters ↑	*Datum ↑*
Name des Beauftragten des Dienstanbieters ↑	*Titel ↑*

Vertretenes Dienstanbieterunternehmen ↑

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen Konformitätsstatus für jede Anforderung aus. Wenn Sie eine der Anforderungen mit „NEIN“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung voraussichtlich erfüllen wird. Geben Sie außerdem eine kurze Beschreibung der Aktionen an, die unternommen werden, um die Anforderung zu erfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

[5] Im Magnetstreifen verschlüsselte Daten oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Spurdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

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

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

PCI-DSS-Anforderung	Anforderungsbeschreibung	Konformitätsstatus (eine Option auswählen)		Abhilfedatum und Aktionen (bei Konformitätsstatus „NEIN“)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	☐	☐	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	☐	☐	
3	Schutz gespeicherter Karteninhaberdaten	☐	☐	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	☐	☐	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	☐	☐	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	☐	☐	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf	☐	☐	
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	☐	☐	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	☐	☐	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	☐	☐	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	☐	☐	
12	Pflegen einer Informationssicherheitsrichtlinie für das gesamte Personal	☐	☐	

Selbstbeurteilungsfragebogen D

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

Ausfülldatum:

Erstellung und Wartung eines sicheren Netzwerks

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

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
1.1	Wurden Standards für die Firewall- und Router-Konfiguration festgelegt, die folgende Elemente beinhalten?				
1.1.1	Gibt es einen offiziellen Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration?		☐	☐	
1.1.2	(a) Gibt es ein aktuelles Netzwerkdiagramm (z. B. ein Diagramm, das Flüsse von Karteninhaberdaten im Netzwerk darstellt), das alle Verbindungen mit Karteninhaberdaten dokumentiert, einschließlich aller drahtlosen Netzwerke?		☐	☐	
	(b) Wird das Diagramm regelmäßig aktualisiert?		☐	☐	
1.1.3	(a) Enthalten alle Standards für die Firewall-Konfiguration Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone?		☐	☐	
	(b) Entspricht das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration?		☐	☐	
1.1.4	Enthalten Standards für die Firewall- und Router-Konfiguration eine Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten?		☐	☐	
1.1.5	(a) Enthalten Standards für die Firewall- und Router-Konfiguration eine dokumentierte Liste mit Services, Protokollen und Ports, die für die Geschäftsausübung erforderlich sind, z. B. Hypertext Transfer Protocol (HTTP) und Secure Sockets Layer (SSL), Secure Shell (SSH) und Virtual Private Network (VPN)?		☐	☐	
	(b) Sind alle zulässigen unsicheren Services, Protokolle und Ports erforderlich und sind die jeweiligen Sicherheitsfunktionen hierfür einzeln dokumentiert und implementiert? *Hinweis: Beispiele für unsichere Dienste, Protokolle oder Ports sind unter anderem FTP, Telnet, POP3, IMAP und SNMP.*		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	1.1.6	(a) Erfordern die Standards für die Firewall- und Router-Konfiguration mindestens alle sechs Monate eine Prüfung von Firewall- und Router-Regeln?	☐	☐	
		(b) Werden die Firewall- und Router-Regeln mindestens alle sechs Monate überprüft?	☐	☐	
1.2	Schränken die Firewall- und Router-Konfigurationen die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und sämtlichen Systemen in der Karteninhaberdaten-Umgebung wie folgt ein? *Hinweis: Ein „nicht vertrauenswürdiges Netzwerk" ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Stelle gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Stelle liegt.*				
	1.2.1	(a) Wird der ein- und ausgehende Netzwerkverkehr auf den für die Karteninhaberdaten-Umgebung notwendigen Verkehr beschränkt und sind diese Beschränkungen dokumentiert?	☐	☐	
		(b) Wird der restliche ein- und ausgehende Verkehr eigens abgelehnt (z. B. durch die Verwendung einer ausdrücklichen „Alle ablehnen"-Anweisung oder einer impliziten Anweisung zum Ablehnen nach dem Zulassen)?	☐	☐	
	1.2.2	Sind die Router-Konfigurationsdateien sicher und synchronisiert?	☐	☐	
	1.2.3	Sind zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung Umkreis-Firewalls installiert und sind diese Firewalls so konfiguriert, dass der gesamte Verkehr aus der drahtlosen Umgebung entweder abgelehnt oder kontrolliert wird (sofern dieser Verkehr für Geschäftszwecke notwendig ist)?	☐	☐	
1.3	Verbietet die Firewall-Konfiguration wie folgt den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung?				
	1.3.1	Ist eine DMZ implementiert, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich erhältliche Dienste, Protokolle und Ports anbieten?	☐	☐	
	1.3.2	Ist der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt?	☐	☐	
	1.3.3	Werden direkt eingehende oder ausgehende Verbindungen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung untersagt?	☐	☐	
	1.3.4	Ist die Weiterleitung interner Adressen aus dem Internet in die DMZ verboten?	☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	1.3.5	Ist die Weiterleitung ausgehenden Datenverkehrs von der Karteninhaberdaten-Umgebung an das Internet ausdrücklich erlaubt?	☐	☐	
	1.3.6	Ist eine zustandsorientierte Inspektion, auch Dynamic Packet Filtering genannt, implementiert (d. h. nur „etablierte“ Verbindungen können in das Netzwerk gelangen)?	☐	☐	
	1.3.7	Sind Systemkomponenten, die Karteninhaberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone gespeichert, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist?	☐	☐	
	1.3.8	(a) Wurden Methoden implementiert, um die Offenlegung privater IP-Adressen und Routing-Informationen an das Internet zu verhindern? ***Hinweis**: Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderem:* • *Network Address Translation (NAT);* • *Das Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls oder Inhalts-Caches;* • *Löschen oder Filtern von Route-Advertisements für private Netzwerke, die registrierte Adressen verwenden;* • *Interne Nutzung eines RFC1918-Adressraums anstatt registrierter Adressen.*	☐	☐	
		(b) Dürfen private IP-Adressen und Routing-Informationen an externe Stellen weitergegeben werden?	☐	☐	
1.4	(a)	Ist eine persönliche Firewallsoftware auf allen mobilen und Mitarbeitern gehörenden Computern mit direkter Verbindung zum Internet installiert (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden?	☐	☐	
	(b)	Wurde die persönliche Firewallsoftware vom Unternehmen gemäß bestimmter Standards konfiguriert und ist diese durch Benutzer mobiler Computer und/oder Computer von Mitarbeitern veränderbar?	☐	☐	

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

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
2.1	Werden vom Anbieter gelieferte Standardeinstellungen immer geändert, bevor ein System im Netzwerk installiert wird? *Zu den vom Anbieter angegebenen Standardeinstellungen gehören u. a. Kennwörter, SNMP-Community-Zeichenfolgen und nicht benötigte Konten.*		☐	☐	
2.1.1	Für drahtlose Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder die Karteninhaberdaten übertragen, werden die Standardeinstellungen wie folgt geändert?				
	(a) Werden Standardwerte der Verschlüsselungsschlüssel zum Zeitpunkt der Installation geändert und werden sie jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt?		☐	☐	
	(b) Werden Standard-SNMP-Community-Zeichenfolgen auf drahtlosen Geräten geändert?		☐	☐	
	(c) Werden Standardkennwörter/-sätze auf Zugriffspunkten geändert?		☐	☐	
	(d) Wird die Firmware auf drahtlosen Geräten aktualisiert, um eine starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen?		☐	☐	
	(e) Werden gegebenenfalls auch andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen geändert?		☐	☐	
2.2	(a) Werden für alle Systemkomponenten Konfigurationsstandards entwickelt und sind diese mit den branchenüblichen Systemhärtungsstandards vereinbar? Zu den Quellen für branchenübliche Systemhärtungsstandards gehören u. a. SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) und Center for Internet Security (CIS).		☐	☐	
	(b) Werden die Systemkonfigurationsstandards gemäß Anforderung 6.2 aktualisiert, sobald neue Schwachstellen identifiziert werden?		☐	☐	
	(c) Werden neue Systemkonfigurationsstandards angewendet, sobald neue Systeme konfiguriert werden?		☐	☐	
	(d) Umfassen die festgelegten Konfigurationsstandards folgende Punkte?				

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	2.2.1	(a) Ist nur eine primäre Funktion pro Server implementiert, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveauanforderungen existieren? (Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.)	☐	☐	
		(b) Wenn Virtualisierungstechnologien eingesetzt werden, ist pro virtuelle Systemkomponente oder Gerät nur eine primäre Funktion implementiert?	☐	☐	
	2.2.2	(a) Werden für den Betrieb des Systems nur notwendige Dienste, Protokolle, Daemons usw. aktiviert (d. h. nicht direkt für die Ausführung der spezifischen Gerätefunktion erforderliche Funktionen werden deaktiviert)?	☐	☐	
		(b) Werden alle aktivierten unsicheren Services, Daemons oder Protokolle begründet und Sicherheitsfunktionen einzeln dokumentiert und implementiert? *(Es werden zum Beispiel gesicherte Technologien wie etwa SSH, S-FTP, SSL oder IPSec VPN verwendet, um unsichere Dienste wie beispielsweise NetBIOS, File-Sharing, Telnet, FTP usw. zu schützen.)*	☐	☐	
	2.2.3	(a) Verstehen sich Systemadministratoren und/oder Mitarbeiter, die Systemkomponenten konfigurieren, auf allgemeine Sicherheitsparametereinstellungen für diese Systemkomponenten?	☐	☐	
		(b) Sind in den Systemkonfigurationsstandards gängige Sicherheitsparametereinstellungen enthalten?	☐	☐	
		(c) Sind die Sicherheitsparametereinstellungen auf den Systemkomponenten sachgemäß eingestellt?	☐	☐	
	2.2.4	(a) Wurden alle unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver entfernt?	☐	☐	
		(b) Werden aktivierte Funktionen dokumentiert und sind sie sicher konfiguriert?	☐	☐	
		(c) Sind auf den Systemkomponenten ausschließlich dokumentierte Funktionen vorhanden?	☐	☐	
2.3	Ist der Nichtkonsolen-Verwaltungszugriff wie folgt verschlüsselt? *Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff*				
	(a) Werden alle Nichtkonsolen-Verwaltungszugriffe mit einer starken Kryptographie verschlüsselt und wird eine starke Verschlüsselungsmethode aufgerufen, bevor das Administratorkennwort angefordert wird?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	(b) Sind die Systemdienste und -parameterdateien so konfiguriert, dass die Nutzung von Telnet und anderen unsicheren Remote-Anmeldebefehlen verhindert wird?		☐	☐	
	(c) Ist der Administratorzugriff auf die webbasierten Managementschnittstellen mit einer starken Kryptographie verschlüsselt?		☐	☐	
2.4	Falls Sie ein Hosting-Anbieter sind, sind Ihre Systeme so konfiguriert, dass die gehostete Umgebung und die Karteninhaberdaten jeder Stelle geschützt werden? *Siehe* Anhang A: Zusätzliche PCI-DSS-Anforderungen für gemeinsam verwendete Hosting-Provider *für spezifische Anforderungen, die erfüllt werden müssen.*		☐	☐	

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
3.1	Umfassen die Richtlinien und Verfahren zur Datenaufbewahrung und zum Löschen von Daten folgende Punkte?				
3.1.1	(a) Wurden Richtlinien und Verfahren zur Datenaufbewahrung und zum Löschen von Daten implementiert und umfassen diese spezifische Anforderungen bezüglich der Speicherung von Karteninhaberdaten aus geschäftlichen, rechtlichen und/oder gesetzlichen Zwecken? *Karteninhaberdaten müssen z. B. für den Zeitraum X aus den Geschäftsgründen Y aufbewahrt werden.*		☐	☐	
	(b) Enthalten Richtlinien und Verfahren Bestimmungen zum sicheren Löschen von Daten, wenn diese nicht mehr aus rechtlichen, gesetzlichen oder geschäftlichen Gründen benötigt werden, einschließlich des Löschens von Karteninhaberdaten?		☐	☐	
	(c) Decken die Richtlinien und Verfahren alle Aspekte zum Speichern von Karteninhaberdaten ab?		☐	☐	
	(d) Beinhalten die Richtlinien und Verfahren mindestens einen der folgenden Aspekte? • Einen programmatischen (automatischen oder manuellen) Prozess zum mindestens vierteljährlichen Löschen gespeicherter Karteninhaberdaten, die den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschritten haben. • Anforderungen für eine mindestens vierteljährliche Überprüfung dahingehend, ob die gespeicherten Karteninhaberdaten nicht den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschreiten.		☐	☐	
	(e) Erfüllen alle gespeicherten Karteninhaberdaten die in der Datenaufbewahrungsrichtlinie beschriebenen Anforderungen?		☐	☐	
3.2	(a) Geben Kartenemittenten und/oder Unternehmen, die Ausstellungsdienste unterstützen und vertrauliche Authentifizierungsdaten speichern, eine Begründung für die Speicherung dieser vertraulichen Authentifizierungsdaten an und werden die Daten sicher gespeichert?		☐	☐	
	(b) Gibt es bei allen anderen Stellen, falls vertrauliche Authentifizierungsdaten empfangen und gelöscht werden, Prozesse zum Löschen der Daten, um sicherzustellen, dass die Daten nicht wiederhergestellt werden können?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	Halten alle Systeme die folgenden Anforderungen hinsichtlich des Verbots, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern, ein (auch wenn diese verschlüsselt sind)?				
3.2.1	Wird der gesamte Inhalt einer Spur auf dem Magnetstreifen (auf der Rückseite einer Karte, gleichwertige Daten auf einem Chip oder an einer anderen Stelle) tatsächlich nicht gespeichert? Diese Daten werden auch als Full Track, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet. *Hinweis: Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:* ▪ *Der Name des Karteninhabers,* ▪ *Primäre Kontonummer (PAN),* ▪ *Ablaufdatum und* ▪ *Servicecode* *Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.*		☐	☐	
3.2.2	Wird der Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte) tatsächlich nicht gespeichert?		☐	☐	
3.2.3	Werden persönliche Identifizierungsnummern (PIN) oder verschlüsselte PIN-Blocks tatsächlich nicht gespeichert?		☐	☐	
3.3	Ist die PAN bei der Anzeige maskiert (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden)? *Hinweise:* ▪ *Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die die vollständige PAN aus betrieblichen Gründen einsehen müssen.* ▪ *Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. für POS-Belege.*		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
3.4	Wird die PAN mithilfe eines der folgenden Verfahren überall dort unleserlich gemacht, wo sie gespeichert wird (auch auf Daten-Repositories, tragbaren digitalen Medien, Sicherungsmedien und in Audit-Protokollen)? ▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden); ▪ Abkürzung (die Hash-Funktion kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen); ▪ Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden); ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren. *Hinweis: Für eine Person mit böswilligen Absichten ist es eine relativ einfache Übung, die originalen PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die abgekürzte als auch auf die Hash-Version einer PAN hat. Wenn die gehashte und die abgekürzte Version derselben PAN in der Umgebung derselben Stelle nebeneinander bestehen, müssen zusätzliche Kontrollen eingesetzt werden, um sicherzustellen, dass gehashte und abgekürzte Versionen nicht verglichen werden können, um die originale PAN zu rekonstruieren.*		☐	☐	
3.4.1	Falls Datenträgerverschlüsselung (statt der Verschlüsselung auf Datei- oder Datenbankspaltenebene) verwendet wird, wird der Zugriff wie folgt verwaltet:				
	(a) Wird der logische Zugriff auf verschlüsselte Dateisysteme unabhängig von nativen Zugriffskontrollmechanismen des Betriebssystems verwaltet (z. B. indem keine lokalen Benutzerkontodatenbanken verwendet werden)?		☐	☐	
	(b) Werden kryptographische Schlüssel sicher gespeichert (z. B. auf austauschbaren Datenträgern, die durch starke Zugriffskontrollen entsprechend geschützt sind)?		☐	☐	
	(c) Werden Karteninhaberdaten auf austauschbaren Datenträgern unabhängig vom Speicherort verschlüsselt? ***Hinweis**: Wenn keine Datenträgerverschlüsselung zur Verschlüsselung austauschbarer Datenträger eingesetzt wird, müssen die auf diesen Datenträgern gespeicherten Daten mithilfe einer anderen Methode verschlüsselt werden.*		☐	☐	
3.5	Werden wie folgt Schlüssel verwendet, um die Karteninhaberdaten vor Weitergabe und Missbrauch zu schützen? ***Hinweis**: Diese Anforderung gilt auch für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von Schlüsseln zum Verschlüsseln von Daten verwendet werden. Diese Schlüssel zum Verschlüsseln von Schlüsseln müssen mindestens so sicher wie der Schlüssel zum Verschlüsseln von Daten sein.*				

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	3.5.1	Ist der Zugriff auf kryptographische Schlüssel auf die geringstmögliche Anzahl von Wächtern beschränkt?	☐	☐	
	3.5.2	(a) Werden Schlüssel in verschlüsseltem Format gespeichert und werden Schlüssel zum Verschlüsseln von Schlüsseln getrennt von Schlüsseln zum Verschlüsseln von Daten aufbewahrt?	☐	☐	
		(b) Werden kryptographische Schlüssel sicher an möglichst wenigen Speicherorten und in möglichst wenigen Formen gespeichert?	☐	☐	
3.6		(a) Werden alle Schlüsselverwaltungsprozesse und -verfahren für die zur Verschlüsselung von Karteninhaberdaten verwendeten kryptographischen Schlüssel vollständig dokumentiert und implementiert?	☐	☐	
		(b) Nur für Dienstanbieter: Wenn gemeinsam mit Kunden verwendete Schlüssel für die Übertragung oder Speicherung von Karteninhaberdaten verwendet werden, werden den Kunden entsprechend den Anforderungen 3.6.1 bis 3.6.8 unten Dokumentationen bereitstellt, die Anweisungen zur sicheren Übertragung, Speicherung und Aktualisierung von Kundenschlüsseln enthalten?	☐	☐	
		(c) Umfassen die implementierten Schlüsselverwaltungsprozesse und -verfahren folgende Punkte?			
	3.6.1	Umfassen die Verfahren für kryptographische Schlüssel die Generierung starker kryptographischer Schlüssel?	☐	☐	
	3.6.2	Umfassen die Verfahren für kryptographische Schlüssel die Verteilung sicherer kryptographischer Schlüssel?	☐	☐	
	3.6.3	Umfassen die Verfahren für kryptographische Schlüssel die sichere Speicherung kryptographischer Schlüssel?	☐	☐	
	3.6.4	Umfassen die Verfahren für kryptographische Schlüssel Änderungen kryptographischer Schlüssel für Schlüssel, die das Ende ihrer Schlüssellebensdauer erreicht haben (z. B. nach Ablauf einer festgelegten Zeitspanne und/oder nachdem von einem bestimmten Schlüssel eine gegebene Menge an Geheimtext generiert wurde), so wie von dem entsprechenden Anwendungsanbieter oder Schlüsselinhaber definiert und von bewährten Branchenverfahren und -richtlinien vorgegeben (z. B. NIST Special Publication 800-57)?	☐	☐	
	3.6.5	(a) Umfassen die Verfahren für kryptographische Schlüssel die Entfernung oder den Austausch kryptographischer Schlüssel (z. B. mittels Archivierung, Vernichtung und/oder Rückruf), wenn die Integrität des Schlüssels gefährdet ist (z. B. nach Ausscheiden eines Mitarbeiters, der einen Klartext-Schlüssel kennt)?	☐	☐	

PCI-DSS Frage		Antwort:	Ja	Nein	Spezial*
	(b)	Umfassen die Verfahren für kryptographische Schlüssel den Austausch von Schlüsseln, bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden?	☐	☐	
	(c)	Wenn entfernte oder ausgetauschte kryptographische Schlüssel aufbewahrt werden, werden diese Schlüssel ausschließlich für Entschlüsselungs-/Überprüfungszwecke verwendet?	☐	☐	
3.6.6		Umfassen die Verfahren für kryptographische Schlüssel eine geteilte Kenntnis und doppelte Kontrollen kryptographischer Schlüssel (z. B. zwei oder drei Personen, die jeweils nur ihren eigenen Bestandteil des Schlüssels kennen, um den gesamten Schlüssel neu zu erstellen) für manuelle Verfahren zur Schlüsselverwaltung von Klartext-Schlüsseln? ***Hinweis**: Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen: Schlüsselgenerierung, Übertragung, Ladung, Speicherung und Vernichtung.*	☐	☐	
3.6.7		Umfassen die Verfahren für kryptographische Schlüssel Verfahren zur Prävention nicht autorisierter Ersetzungen kryptographischer Schlüssel?	☐	☐	
3.6.8		Müssen Wächter kryptographischer Schlüssel formal bestätigen (entweder schriftlich oder elektronisch), dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen?	☐	☐	

Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
4.1	(a) Werden eine starke Kryptographie und Sicherheitsprotokolle wie SSL/TLS, SSH oder IPSEC eingesetzt, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen? *Beispiele offener, öffentlicher Netzwerke im Rahmen des PCI-DSS sind das Internet, Wireless-Technologien, das Global System for Mobile Communications (GSM) und der General Packet Radio Service (GPRS).*		☐	☐	
	(b) Werden ausschließlich vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert?		☐	☐	
	(c) Sind Sicherheitsprotokolle implementiert, um ausschließlich sichere Konfigurationen zu verwenden und keine unsicheren Versionen oder Konfigurationen zu unterstützen?		☐	☐	
	(d) Wird für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet (siehe Anbieterempfehlungen/bewährte Verfahren)?		☐	☐	
	(e) Für SSL/TLS-Implementierungen: • Wird HTTPS als Bestandteil der Browser-URL (Universal Record Locator) angezeigt? • Sind Karteninhaberdaten nur erforderlich, wenn in der URL HTTPS angezeigt wird?		☐	☐	
	4.1.1 Werden bewährte Branchenverfahren (z. B. IEEE 802.11i) eingesetzt, um eine starke Verschlüsselung in der Authentifizierung und Übertragung für drahtlose Netzwerke zu implementieren, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind? ***Hinweis**: Die Nutzung von WEB als Sicherheitskontrolle ist seit dem 30. Juni 2010 untersagt.*		☐	☐	
4.2	(a) Werden PANs unleserlich gemacht oder mit einer starken Kryptographie gesichert, wenn sie über Messaging-Technologien für Endanwender gesendet werden (z. B. per E-Mail, Instant Messaging oder Chat)?		☐	☐	
	(b) Sind Richtlinien vorhanden, die festlegen, dass ungeschützte PANs nicht über Messaging-Technologien für Endanwender gesendet werden dürfen?		☐	☐	

Unterhaltung eines Anfälligkeits-Managementprogramms

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
5.1	Ist eine Virenschutzsoftware auf allen Systemen, die üblicherweise das Ziel böswilliger Software sind, implementiert?		☐	☐	
5.1.1	Sind alle Virenschutzprogramme in der Lage, bekannte Malware-Typen (z. B. Viren, Trojaner, Würmer, Spyware, Adware und Rootkits) zu erkennen, zu entfernen und vor ihnen zu schützen?		☐	☐	
5.2	Werden alle Antivirenprogramme regelmäßig aktualisiert, aktiv ausgeführt und generieren sie Audit-Protokolle?				
	(a) Erfordert die Virenschutzrichtlinie die Aktualisierung von Antivirussoftware und -definitionen?		☐	☐	
	(b) Ist die Master-Installation der Software für automatische Updates und regelmäßige Scans aktiviert?		☐	☐	
	(c) Sind automatische Updates und regelmäßige Scans aktiviert?		☐	☐	
	(d) Generieren alle Virenschutzmechanismen Audit-Protokolle und werden die Protokolle gemäß PCI-DSS-Anforderung 10.7 aufbewahrt?		☐	☐	

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
6.1	(a) Werden alle Systemkomponenten und Softwareanwendungen vor bekannten Sicherheitslücken mithilfe der neuesten Sicherheitspatches der jeweiligen Hersteller geschützt?		☐	☐	
	(b) Werden wichtige Sicherheitspatches innerhalb eines Monats nach der Freigabe installiert? ***Hinweis**: Ein Unternehmen kann den Einsatz eines risikobasierten Ansatzes in Erwägung ziehen, um seine Patch-Installationen zu priorisieren. Beispielsweise kann kritischer Infrastruktur (z. B. öffentliche Geräte und Systeme, Datenbanken) eine höhere Priorität eingeräumt werden als weniger kritischen internen Geräten, um zu gewährleisten, dass Systeme und Geräte mit hoher Priorität innerhalb eines Monats und weniger kritische Geräte und Systeme innerhalb von drei Monaten adressiert werden.*		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
6.2	(a) Ist ein Prozess vorhanden, um neu entdeckte Sicherheitslücken zu identifizieren und um das Risiko der einzelnen Schwachstellen zu bewerten? (Zumindest die wichtigsten, schwerwiegendsten Schwächen sollten mit „schwerwiegend“ gekennzeichnet werden.) ***Hinweis**: Die Risikobewertungen müssen auf den Best Practices der Branche aufbauen. Ein Kriterium, um eine Schwäche mit einem „schwerwiegenden“ Risiko einzustufen, könnte beispielsweise eine CVSS-Grundbewertung von 4.0 oder höher sein und/oder ein Patch von einem Anbieter, das als „kritisch“ bewertet wird, und/oder eine Schwäche, die eine wichtige Systemkomponente betrifft.* *Die Bewertung von Sicherheitslücken wird bis 30. Juni 2012 als Best Practices angesehen, danach wird sie zu einer Anforderung.*		☐	☐	
	(b) Umfassen Prozesse zum Identifizieren neuer Sicherheitslücken die Verwendung von externen Quellen für Informationen zu Sicherheitslücken?		☐	☐	
6.3	(a) Basieren die Softwareentwicklungsprozesse auf Branchenstandards und/oder Best Practices?		☐	☐	
	(b) Ist die Informationssicherheit durchweg über den gesamten Softwareentwicklungszyklus integriert?		☐	☐	
	(c) Werden Softwareanwendungen gemäß dem PCI-DSS entwickelt (z. B. sichere Authentifizierung und Protokollierung)?		☐	☐	
	(d) Gewährleisten die Softwareentwicklungsprozesse folgende Punkte?				
6.3.1	Werden benutzerdefinierte Anwendungskonten, Benutzernamen und Kennwörter gelöscht, bevor Anwendungen aktiv oder an Kunden freigegeben werden?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	6.3.2	Werden alle benutzerdefinierten Programmcodeänderungen vor der Freigabe an die Produktion oder an Kunden überprüft (entweder mithilfe manueller oder automatischer Prozesse), um alle potenziellen Programmanfälligkeiten wie folgt zu identifizieren? • Werden Codeänderungen von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes sowie von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind? • Gewährleisten die Codeprüfungen, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird (siehe PCI-DSS-Anforderung 6.5)? • Werden vor der Freigabe entsprechende Korrekturen implementiert? • Werden die Ergebnisse der Codeprüfung vor der Freigabe vom Management geprüft und genehmigt? ***Hinweis**: Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus. Code-Prüfungen können von qualifiziertem internen Personal oder von Dritten ausgeführt werden. Webanwendungen unterliegen auch zusätzlichen Kontrollen, wenn sie öffentlich sind, um laufende Bedrohungen und Sicherheitslücken nach der Implementierung gemäß der Definition in PCI-DSS-Anforderung 6.6 zu beheben.*	☐	☐	
6.4		Werden Änderungskontrollprozesse und -verfahren für alle Änderungen an Systemkomponenten befolgt, um die nachstehenden Aspekte abzudecken?			
	6.4.1	Sind die Entwicklungs-/Testumgebungen von der Produktionsumgebung getrennt, und ist zum Durchsetzen dieser Trennung eine Zugriffssteuerung implementiert?	☐	☐	
	6.4.2	Gibt es zwischen den Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und den Mitarbeitern, die der Produktionsumgebung zugeteilt sind, eine Aufgabentrennung?	☐	☐	
	6.4.3	Werden Produktionsdaten (Live-PANs) tatsächlich ***nicht*** zum Testen oder in der Entwicklung verwendet?	☐	☐	
	6.4.4	Werden Testdaten und -konten entfernt, bevor Produktionssysteme aktiv werden?	☐	☐	
	6.4.5	(a) Werden die Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen dokumentiert und setzen sie die Punkte 6.4.5.1-6.4.5.4 unten voraus?	☐	☐	
		(b) Werden bei allen Änderungen die folgenden Schritte ausgeführt?			

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	6.4.5.1	Dokumentation der Auswirkungen;	☐	☐	
	6.4.5.2	Dokumentation der Genehmigung durch autorisierte Parteien;	☐	☐	
	6.4.5.3	(a) Funktionstests, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.	☐	☐	
		(b) Werden bei benutzerspezifischen Codeänderungen Updates auf ihre Konformität mit der PCI-DSS-Anforderung 6.5 getestet, bevor sie in der Produktionsumgebung implementiert werden?	☐	☐	
	6.4.5.4	Werden Back-Out-Verfahren für jede Änderung vorbereitet?	☐	☐	
6.5		(a) Werden alle Anwendungen anhand sicherer Programmierungsrichtlinien entwickelt? (Z. B. *der Open Web Application Security Project (OWASP) Leitfaden, SANS CWE Top 25, CERT Secure Coding usw.*)?	☐	☐	
		(b) Kennen sich die Entwickler mit sicheren Codierungsverfahren aus?	☐	☐	
		(c) Wird die Vorbeugung häufiger Programmierungsanfälligkeiten in Softwareentwicklungsprozessen berücksichtigt, um sicherzustellen, dass die Anwendungen mindestens nicht von folgenden Schwachstellen bedroht sind? *Hinweis: Die unter 6.5.1 bis 6.5.9 aufgeführten Schwachstellen entsprachen zum Zeitpunkt der Veröffentlichung dieser Version des PA-DSS den Best Practices der Branche. Da jedoch die Best Practices der Branche im Anfälligkeits-Management aktualisiert werden, müssen für diese Anforderungen die aktuellen Best Practices verwendet werden.*			
	6.5.1	Injektionsfehler, insbesondere bei der SQL-Injektion? (Validieren Sie die Eingabe, um zu überprüfen, ob Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern und parametrisierte Abfragen verwenden können usw.) *Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.*	☐	☐	
	6.5.2	Pufferüberlauf? (Validieren von Puffergrenzen und Kürzen von Eingabestrings.)	☐	☐	
	6.5.3	Unsichere kryptographische Speicher? (Verhindern Sie kryptographische Fehler.)	☐	☐	
	6.5.4	Unsichere Mitteilungen? (Verschlüsseln Sie alle authentifizierten und vertraulichen Mitteilungen ordnungsgemäß.)	☐	☐	
	6.5.5	Inkorrekte Fehlerhandhabung? (Geben Sie keine Informationen über Fehlermeldungen preis.)	☐	☐	

	PCI-DSS Frage		Antwort:	Ja	Nein	Spezial*
	6.5.6	Werden alle „schwerwiegenden“ Schwachstellen entsprechend des Identifikationsprozesses von Schwächen dargelegt (wie in der PCI-DSS-Anforderung 6.2 definiert)? ***Hinweis**: Diese Anforderung wird bis zum 30. Juni 2012 als Best Practice angesehen, danach wird sie zu einer Anforderung.*		☐	☐	
	Für Web-Anwendungen und Anwendungsschnittstellen (intern und extern) werden darüber hinaus die folgenden zusätzlichen Schwachstellen angesprochen:					
	6.5.7	Siteübergreifendes Scripting (XSS) (Validierung aller Parameter vor der Aufnahme, Verwendung einer kontextspezifischen Außerkraftsetzungsfunktion usw.)		☐	☐	
	6.5.8	Kontrolle unangemessener Zugriffe wie unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal (Angemessene Authentifizierung von Benutzern und Eingabebereinigung. Machen Sie interne Objektverweise Benutzern nicht zugänglich.)		☐	☐	
	6.5.9	Cross-Site Request Forgery (CSRF) (Antworten Sie nicht auf Autorisierungsinformationen und Tokens, die automatisch von Browsern gesendet werden.)		☐	☐	
6.6	Werden alle öffentlichen Webanwendungen regelmäßig von neuen Bedrohungen und Schwachstellen befreit und werden diese Anwendungen vor bekannten Angriffen geschützt, indem *eine* der folgenden Methoden angewendet wird? ▪ Überprüfungen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit: o Mindestens jährlich o Nach jeder Änderung o Durch ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist o Dass alle Sicherheitslücken geschlossen werden o Dass die Anwendung nach den Korrekturen erneut bewertet wird *– oder –* ▪ Installation einer Webanwendungs-Firewall vor öffentlichen Webanwendungen, um webbasierte Angriffe zu erkennen und zu verhindern. ***Hinweis**: „Ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist“, kann ein Drittunternehmen oder eine interne Organisation sein, sofern sich die Prüfer auf Anwendungssicherheit spezialisieren und die Unabhängigkeit vom Entwicklungsteam nachweisen können.*			☐	☐	

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
7.1	Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten wie folgt ausschließlich auf jene Personen beschränkt, deren Tätigkeit diesen Zugriff erfordert?				
7.1.1	Sind die Zugriffsrechte für Benutzernamen auf Mindestberechtigungen beschränkt, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind?		☐	☐	
7.1.2	Werden Berechtigungen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen (auch als „rollenbasierte Zugriffssteuerung“ oder RBAC bezeichnet)?		☐	☐	
7.1.3	Sind dokumentierte Genehmigungen autorisierter Parteien erforderlich (schriftlich oder elektronisch), in denen die erforderlichen Berechtigungen angegeben werden?		☐	☐	
7.1.4	Wurden die Zugriffskontrollen über ein automatisiertes Zugriffskontrollsystem implementiert?		☐	☐	
7.2	Besteht für Systeme mit mehreren Benutzern ein Zugriffskontrollsystem, um den Zugriff anhand des Informationsbedarfs eines Benutzers zu beschränken, und ist dieses System wie folgt auf „Alle ablehnen“ eingestellt, sofern der Zugriff nicht ausdrücklich genehmigt wurde?				
7.2.1	Wurden auf allen Systemkomponenten Zugriffskontrollsysteme implementiert?		☐	☐	
7.2.2	Wurden die Zugriffskontrollsysteme konfiguriert, um Berechtigungen durchzusetzen, die einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen sind?		☐	☐	
7.2.3	Weisen die Zugriffskontrollsysteme die Standardeinstellung „Alle ablehnen“ auf? ***Hinweis**: Einige Zugriffskontrollsysteme sind standardmäßig auf „Alle zulassen“ gesetzt und lassen dadurch den Zugriff zu, bis eine Regel erstellt wird, die den Zugriff ausdrücklich ablehnt.*		☐	☐	

Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
8.1	Wurde allen Benutzern eine eindeutige Benutzer-ID zugewiesen, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wurde?		☐	☐	
8.2	Werden neben der Zuweisung einer eindeutigen ID eine oder mehrere der folgenden Methoden eingesetzt, um alle Benutzer zu authentifizieren? ▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; ▪ Etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; ▪ Etwas, das Sie sind, wie zum Beispiel biometrische Daten.		☐	☐	
8.3	Wurde eine Authentifizierung anhand zweier Faktoren für den Remote-Zugriff auf das Netzwerk (Netzwerkzugriff von außerhalb des Netzwerks) durch Mitarbeiter, Administratoren und Dritten eingeführt? *(z. B. Remote-Authentifizierung und Einwählдienst (RADIUS) mit Tokens; Terminal Access Controller Access Control System (TACACS) mit Tokens oder andere Technologien, die eine Authentifizierung anhand zweier Faktoren unterstützen.)* ***Hinweis**: Bei der Authentifizierung anhand zweier Faktoren müssen zwei der drei Authentifizierungsmethoden (siehe PCI-DSS-Anforderung 8.2 für eine Beschreibung der Authentifizierungsmethoden) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Authentifizierung anhand zweier Faktoren.*		☐	☐	
8.4	(a) Werden alle Kennwörter während dem Speichern und der Übertragung auf sämtlichen Systemkomponenten unter Verwendung einer starken Kryptographie unleserlich gemacht?		☐	☐	
	(b) Nur für Dienstanbieter: Werden Kundenkennwörter verschlüsselt?		☐	☐	
8.5	Wurden wie folgt entsprechende Benutzerauthentifizierungs- und Authentifizierungsverwaltungskontrollen für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten implementiert?				
8.5.1	Werden Erweiterungen, Löschungen oder Änderungen von Benutzer-IDs, Berechtigungen oder anderen Identifizierungsobjekten kontrolliert, sodass Benutzer-IDs nur im Rahmen ihrer zugehörigen Genehmigung implementiert werden (einschließlich der angegebenen Rechte)?		☐	☐	
8.5.2	Wird die Identität des Benutzers überprüft, bevor ein Kennwort auf Anfrage des Benutzers zurückgesetzt wird (falls die Anfrage per Telefon, E-Mail oder über das Internet erfolgt ist)?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
8.5.3	Werden Kennwörter für die erstmalige Systemverwendung sowie zurückgesetzte Kennwörter für jeden Benutzer auf einen eindeutigen Wert gesetzt, und muss jeder Benutzer sein Kennwort sofort nach der ersten Verwendung ändern?		☐	☐	
8.5.4	Wird der Zugriff ehemaliger Benutzer sofort deaktiviert oder entfernt?		☐	☐	
8.5.5	Werden Benutzerkonten, die über einen Zeitraum von über 90 Tagen inaktiv waren, entfernt oder deaktiviert?		☐	☐	
8.5.6	(a) Sind die von Anbietern für den Remote-Zugriff, Wartungsarbeiten oder den Support verwendeten Konten ausschließlich während des erforderlichen Zeitraums aktiviert?		☐	☐	
	(b) Werden die Konten von Anbietern für den Remote-Zugriff überwacht, wenn sie in Verwendung sind?		☐	☐	
8.5.7	Werden Authentifizierungsverfahren und -richtlinien allen Benutzern mit Zugriff auf Karteninhaberdaten vermittelt?		☐	☐	
8.5.8	Sind Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden wie folgt untersagt? • Allgemeine Benutzer-IDs und -konten wurden deaktiviert oder entfernt; • Es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen; und • Es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Verwaltung von Systemkomponenten verwendet.		☐	☐	
8.5.9	(a) Werden Benutzerkennwörter mindestens alle 90 Tage geändert?		☐	☐	
	(b) Nur für Dienstanbieter: Müssen Kennwörter von Nichtverbraucherbenutzern regelmäßig geändert werden und werden Nichtverbraucherbenutzern Hinweise dazu gegeben, wann und unter welchen Umständen die Kennwörter geändert werden müssen?		☐	☐	
8.5.10	(a) Ist eine Mindestkennwortlänge von sieben Zeichen obligatorisch?		☐	☐	
	(b) Nur für Dienstanbieter: Müssen Kennwörter von Nichtverbraucherbenutzern bestimmte Mindestlängen erfüllen?		☐	☐	
8.5.11	(a) Müssen Kennwörter sowohl numerische als auch alphabetische Zeichen enthalten?		☐	☐	
	(b) Nur für Dienstanbieter: Müssen Kennwörter von Nichtverbraucherbenutzern sowohl numerische als auch alphabetische Zeichen enthalten?		☐	☐	

PCI-DSS Frage		Antwort:	Ja	Nein	Spezial*
8.5.12	(a)	Muss eine Person ein neues Kennwort einreichen, das sich von den letzten vier Kennwörtern unterscheidet, die sie verwendet hat?	☐	☐	
	(b)	Nur für Dienstanbieter: Müssen sich neue Kennwörter von Nichtverbraucherbenutzern von den letzten vier verwendeten Kennwörtern unterscheiden?	☐	☐	
8.5.13	(a)	Werden wiederholte Zugriffsversuche begrenzt, indem die Benutzer-ID nach mehr als sechs Versuchen gesperrt wird?	☐	☐	
	(b)	Nur für Dienstanbieter: Werden Kennwörter von Nichtverbraucherbenutzern nach mehr als sechs ungültigen Zugriffsversuchen gesperrt?	☐	☐	
8.5.14		Wird die Dauer der Sperre eines Benutzerkontos auf mindestens 30 Minuten festgelegt oder bis die Benutzer-ID durch den Administrator wieder freigeschaltet wird?	☐	☐	
8.5.15		Müssen sich Benutzer nach einer mehr als 15-minütigen Inaktivität erneut authentifizieren (z. B. indem sie das Kennwort erneut eingeben), um das Terminal oder die Sitzung zu reaktivieren?	☐	☐	
8.5.16	(a)	Erfolgt der gesamte Zugriff auf Datenbanken mit Karteninhaberdaten über eine Authentifizierung? (Dies umfasst den Zugriff durch Anwendungen, Administratoren und alle anderen Benutzer.)	☐	☐	
	(b)	Erfolgen sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank (z. B. Verschieben, Kopieren und Löschen) ausschließlich programmgesteuert (z. B. über gespeicherte Verfahren)?	☐	☐	
	(c)	Sind der Direktzugriff oder Datenbankabfragen Datenbankadministratoren vorbehalten?	☐	☐	
	(d)	Können Anwendungs-IDs nur von den Anwendungen (und nicht von Einzelbenutzern oder anderen Prozessen) verwendet werden?	☐	☐	

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
9.1	Wurden angemessene Zugangskontrollen implementiert, um den physischen Zugriff auf Systeme in der Karteninhaberdaten-Umgebung zu überwachen und zu beschränken?		☐	☐	
9.1.1	(a) Wird der Zugang zu zugangsbeschränkten Bereichen mithilfe von Videokameras und/oder Kontrollsystemen überwacht? ***Hinweis**: „Zugangsbeschränkte Bereiche" sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert werden. Hierzu zählen nicht die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).*		☐	☐	
	(b) Sind die Videokameras und/oder Kontrollsysteme vor Manipulation oder Deaktivierung geschützt?		☐	☐	
	(c) Werden die anhand von Videokameras und/oder Kontrollsystemen erfassten Daten überprüft und mit anderen Eingaben verglichen und werden diese Daten mindestens für einen Zeitraum von drei Monaten gespeichert, sofern keine anderweitige gesetzliche Regelung zutrifft?		☐	☐	
9.1.2	Ist der physische Zugriff auf öffentlich zugängliche Netzwerkbuchsen beschränkt (Beispielsweise sollten für Besucher zugängliche Bereiche keine aktiven Netzwerkports haben, sofern der Netzwerkzugriff nicht ausdrücklich zugelassen ist.)? Werden Besucher andernfalls nicht alleine bzw. unbeobachtet in Bereichen mit aktiven Netzwerkbuchsen gelassen?		☐	☐	
9.1.3	Ist der physische Zugriff auf WLAN-Zugriffspunkte, Gateways, Handheld-Geräte, Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen beschränkt?		☐	☐	
9.2	Wurden wie folgt Verfahren entwickelt, die die Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern erleichtern? *Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Mitarbeiter vor Ort" hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und Subunternehmen sowie Berater, die am Standort der jeweiligen Stelle arbeiten. Ein „Besucher" wird als Lieferant, Gast eines Mitarbeiters vor Ort, Servicemitarbeiter oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag.*				

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	(a) Umfassen die Prozesse und Verfahren bezüglich der Vergabe von Ausweisen an das Personal vor Ort und Besucher folgende Punkte? • Ausstellen neuer Ausweise; • Änderung von Zugangs- bzw. Zugriffsanforderungen und • Deaktivierung der Zugangsberechtigung für ausgeschiedene Mitarbeiter vor Ort und bei auslaufendem Besucherstatus.		☐	☐	
	(b) Ist der Zugriff auf das Ausweissystem ausschließlich befugtem Personal vorbehalten?		☐	☐	
	(c) Werden Besucher anhand der Ausweise klar identifiziert und sind sie leicht von den Mitarbeitern vor Ort zu unterscheiden?		☐	☐	
9.3	Wird mit allen Besuchern wie folgt umgegangen:				
9.3.1	Verfügen Besucher vor Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden, über eine entsprechende Genehmigung?		☐	☐	
9.3.2	(a) Wird Besuchern ein physisches Token (z. B. ein Ausweis oder Zugangsgerät) ausgestellt, das sie als solche identifiziert?		☐	☐	
	(b) Haben die Besucherausweise eine begrenzte Gültigkeit?		☐	☐	
9.3.3	Werden die Besucher bei Verlassen der Einrichtung oder bei Auslauf der Zugangserlaubnis gebeten, das physische Token auszuhändigen?		☐	☐	
9.4	(a) Gibt es ein Besucherprotokoll, in dem der Zugang zur Einrichtung sowie zu den Computerräumen und Rechenzentren, in denen Karteninhaberdaten gespeichert oder übertragen werden, protokolliert wird?		☐	☐	
	(b) Enthält das Protokoll den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der den physischen Zugang gewährt hat, und wird das Protokoll mindestens drei Monate aufbewahrt?		☐	☐	
9.5	(a) Werden an einem sicheren Ort, vorzugsweise in einer anderen Einrichtung wie einem alternativen oder Backup-Standort oder einer kommerziellen Lagereinrichtung Medien-Backups aufbewahrt?		☐	☐	
	(b) Wird die Sicherheit dieses Standorts mindestens einmal pro Jahr überprüft?		☐	☐	
9.6	Wird die physische Sicherheit aller Medien gewährleistet (einschließlich, aber nicht beschränkt auf Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)? *Zum Zwecke der Anforderung 9, bezieht sich der Begriff „Medien“ auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.*		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
9.7	(a) Wird die interne oder externe Verteilung jeglicher Art von Medien stets strikt kontrolliert?		☐	☐	
	(b) Umfassen die Kontrollen Folgendes:				
9.7.1	Werden Medien klassifiziert, sodass die Sensibilität der Daten bestimmt werden kann?		☐	☐	
9.7.2	Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?		☐	☐	
9.8	Werden Protokolle geführt, um Medien zurückverfolgen zu können, die aus einem gesicherten Bereich heraus verlagert wurden, und muss für eine solche Verlagerung zunächst die Genehmigung des Managements eingeholt werden (insbesondere wenn Medien an Einzelpersonen verteilt werden)?		☐	☐	
9.9	Werden strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durchgeführt?		☐	☐	
9.9.1	Werden ordnungsgemäß Medieninventurlisten geführt und mindestens einmal jährlich Inventuren der vorhandenen Medien durchgeführt?		☐	☐	
9.10	Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?		☐	☐	
	Erfolgt die Vernichtung von Daten wie nachstehend beschrieben?				
9.10.1	(a) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?		☐	☐	
	(b) Werden Container, die Daten beinhalten, welche gelöscht werden sollen, entsprechend geschützt, um Zugriffe auf diese Inhalte zu vermeiden? (Wird ein Container mit zu vernichtenden Akten beispielsweise durch ein Schloss geschützt, um Zugriffe auf den Inhalt zu vermeiden?		☐	☐	
9.10.2	Werden Karteninhaberdaten auf elektronischen Medien nach Branchenstandards unbrauchbar und nicht wiederherstellbar gemacht bzw. anderweitig unbrauchbar gemacht, indem die Medien vernichtet werden (z. B. durch Entmagnetisierung), damit keine Karteninhaberdaten wiederhergestellt werden können?		☐	☐	

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
10.1	Gibt es einen Prozess zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten (insbesondere des Zugriffs mit Administratorprivilegien wie root) mit jedem einzelnen Benutzer?		☐	☐	
10.2	Werden automatisierte Audit-Trails für alle Systemkomponenten implementiert, um folgende Ereignisse rekonstruieren zu können?				
10.2.1	Alle individuellen Benutzerzugriffe auf Karteninhaberdaten;		☐	☐	
10.2.2	Alle von einer Einzelperson mit root- oder Administratorrechten vorgenommenen Aktionen;		☐	☐	
10.2.3	Zugriff auf alle Audit-Trails;		☐	☐	
10.2.4	Ungültige logische Zugriffsversuche;		☐	☐	
10.2 5	Verwendung von Identifizierungs- und Authentifizierungsmechanismen;		☐	☐	
10.2.6	Initialisierung der Audit-Protokolle;		☐	☐	
10.2.7	Erstellung und Löschen von Objekten auf Systemebene.		☐	☐	
10.3	Werden die folgenden Audit-Trail-Einträge für alle Systemkomponenten für jedes Ereignis aufgezeichnet?				
10.3.1	Benutzeridentifizierung,		☐	☐	
10.3.2	Ereignistyp,		☐	☐	
10.3.3	Datum und Uhrzeit,		☐	☐	
10.3.4	Erfolgs- oder Fehleranzeige,		☐	☐	
10.3.5	Ereignisursprung,		☐	☐	
10.3.6	Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen.		☐	☐	
10.4	(a) Werden alle wichtigen Systemuhren und Zeiten durch den Einsatz von Zeitsynchronisierungstechnologien synchronisiert und werden diese Technologien aktualisiert? ***Hinweis**: Eine Zeitsynchronisierungstechnologie ist beispielsweise das Network Time Protocol (NTP).*		☐	☐	
	(b) Sind folgende Steuerungen für den Empfang, die Verteilung und die Speicherung der Zeit implementiert?				
10.4.1	(a) Empfangen ausschließlich ausgewählte zentrale Zeitserver Zeitsignale von externen Quellen und basieren die Zeitsignale von externen Quellen auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC)?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
		(b) Gewährleisten ausgewählte zentrale Zeitserver im Austausch untereinander eine höchstmögliche Genauigkeit und empfangen andere interne Server die Zeit nur von diesen zentralen Zeitservern?	☐	☐	
	10.4.2	Die Zeitinformationen werden wie folgt geschützt: (a) Ist der Zugriff auf Zeitinformationen ausschließlich Mitarbeitern vorbehalten, die den Zugriff auf Zeitinformationen aus geschäftlichen Gründen benötigen?	☐	☐	
		(b) Werden Änderungen an den Zeiteinstellungen auf wichtigen Systemen protokolliert, überwacht und überprüft?	☐	☐	
	10.4.3	Werden die Zeiteinstellungen von branchenüblichen Zeitquellen empfangen? (Somit wird verhindert, dass böswillige Personen die Uhren ändern können.) Diese Zeitaktualisierungen können mit einem symmetrischen Schlüssel verschlüsselt werden. Außerdem können Zugriffskontrolllisten erstellt werden, aus denen die IP-Adressen der Client-Rechner hervorgehen, die die Zeitaktualisierungen in Anspruch nehmen. (Hierdurch wird die Nutzung nicht autorisierter interner Zeitserver verhindert.)	☐	☐	
10.5		Werden wie folgt Audit-Trails gesichert, sodass sie nicht geändert werden können?			
	10.5.1	Ist die Anzeige der Audit-Trails auf Personen mit arbeitsbedingtem Bedarf beschränkt?	☐	☐	
	10.5.2	Werden die Dateien von Audit-Trails mit Zugriffssteuerungssystemen, räumlicher Trennung und/oder Netzwerktrennung vor unbefugten Änderungen geschützt?	☐	☐	
	10.5.3	Werden Audit-Trail-Dateien unverzüglich auf einem zentralisierten Protokollserver oder auf Medien gesichert, die nur schwer zu manipulieren sind?	☐	☐	
	10.5.4	Werden Protokolle für öffentliche Technologien (z. B. Wireless-Systeme, Firewalls, DNS, E-Mail) auf sicheren, zentralen Protokollservern oder Medien abgelegt bzw. dorthin kopiert?	☐	☐	
	10.5.5	Werden für die Protokolle verschiedene Datei-Integritätsüberwachungs- und Änderungserfassungssoftware verwendet, um zu gewährleisten, dass bestehende Protokolldaten nicht geändert werden können, ohne dass Alarme ausgelöst werden (obgleich neue Daten ohne Auslösung von Alarmen hinzugefügt werden können)?	☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
10.6	Werden Protokolle für alle Systemkomponenten mindestens täglich und eventuelle Ausnahmen sachgemäß überprüft? *Protokollüberprüfungen müssen die Server mit Sicherheitsfunktionen wie Intrusion Detection System (IDS) und Authentication, Authorization and Accounting (AAA)-Protokollserver (z. B. RADIUS) umfassen.* ***Hinweis:** Um die Einhaltung der Anforderung 10.6 zu erzielen, können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.*		☐	☐	
10.7	(a) Wurden Aufbewahrungsrichtlinien und -verfahren für Audit-Protokolle implementiert und setzen diese voraus, dass der Audit-Trail-Verlauf mindestens ein Jahr aufbewahrt wird?		☐	☐	
	(b) Sind Audit-Protokolle mindestens ein Jahr verfügbar und Prozesse zur sofortigen Wiederherstellung von Protokollen mindestens der drei letzten Monate zur Analyse vorhanden?		☐	☐	

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
11.1	(a) Wurde ein dokumentierter Prozess zur vierteljährlichen Erkennung und Identifizierung von Zugriffspunkten für drahtlose Netzwerke implementiert? ***Hinweis**: Methoden, die sich hierfür anbieten, sind unter anderen Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme.* *Welche Methode auch immer verwendet wird, sie muss ausreichend sein, um jegliche nicht autorisierten Geräte zu erkennen und zu identifizieren.*		☐	☐	
	(b) Ist die angewandte Methodik ausreichend, um jegliche nicht autorisierten Zugriffspunkte für drahtlose Netzwerke, einschließlich mindestens folgender Elemente, zu erkennen und zu identifizieren? • In Systemkomponenten eingefügte WLAN-Karten; • An Systemkomponenten angeschlossene tragbare Drahtlosgeräte (z. B. über USB usw.); • An einen Netzwerkport oder ein Netzwerkgerät angeschlossene Drahtlosgeräte.		☐	☐	
	(c) Wird der dokumentierte Prozess zur Identifizierung nicht autorisierter Zugriffspunkte für drahtlose Netzwerke mindestens vierteljährlich auf allen Systemkomponenten und an allen Stellen durchgeführt?		☐	☐	
	(d) Falls eine automatische Überwachung eingesetzt wird (z. B. ein Wireless IDS/IPS-System, NAC usw.), sind in der Konfiguration Alarmmeldungen für das Personal vorgesehen?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	(e) Ist im Vorfallreaktionsplan (Anforderung 12.9) eine Reaktion für den Fall definiert, dass nicht autorisierte drahtlose Geräte entdeckt werden?		☐	☐	
11.2	Werden wie folgt interne und externe Netzwerkanfälligkeits-Scans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Modifizierungen von Firewall-Regeln, Produktupgrades) ausgeführt? ***Hinweis**: Für die anfängliche PCI-DSS-Konformität ist es nicht zwingend erforderlich, dass vier bestandene vierteljährliche Scans abgeschlossen sein müssen, wenn 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Stelle über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle im ersten Scan festgestellten Anfälligkeiten korrigiert wurden, wie ein erneuter Scan beweist. Für die Folgejahre nach der ersten PCI-DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.*				
11.2.1	(a) Werden vierteljährlich interne Schwachstellenprüfungen durchgeführt?		☐	☐	
	(b) Sieht der interne Scanprozess erneute Scans vor, bis der gefundene Fehler behoben wurde oder alle „schwerwiegenden“ Sicherheitslücken wie in der PCI-DSS-Anforderung 6.2 dargelegt gelöst wurden?		☐	☐	
	(c) Werden die internen vierteljährlichen Scans von (einem) dafür qualifizierten internen Mitarbeiter(n) oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?		☐	☐	
11.2.2	(a) Werden vierteljährlich externe Schwachstellenprüfungen durchgeführt?		☐	☐	
	(b) Erfüllen die Ergebnisse des letzten vierteljährlichen externen Scans die Anforderungen des ASV-Programmführers (z. B. keine Schwachstellen, die vom CVSS eine Klassifizierung höher als 4.0 erhalten haben und keine automatischen Ausfälle)?		☐	☐	
	(c) Werden vierteljährliche externe Schwachstellenprüfungen von einem Scanninganbieter (ASV) durchgeführt, der vom Payment Card Industry Security Standards Council (PCI-SSC) zugelassen wurde?		☐	☐	

PCI-DSS Frage		Antwort:	Ja	Nein	Spezial*
11.2.3	(a)	Werden interne und externe Scans nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Modifizierungen von Firewall-Regeln, Produktupgrades) durchgeführt? ***Hinweis**: Nach Netzwerkänderungen durchgeführte Scans können vom internen Personal ausgeführt werden.*	☐	☐	
	(b)	Sieht der Scanprozess erneute Scans vor, bis: • Bei externen Scans keine Sicherheitslücken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung höher als 4.0 bewertet wurden; • Bei internen Scans der Fehler behoben wurde oder alle „schwerwiegenden" Sicherheitslücken wie in der PCI-DSS-Anforderung 6.2 dargelegt gelöst wurden.	☐	☐	
	(c)	Werden die Scans von (einem) dafür qualifizierten internen Mitarbeiter(n) oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	☐	☐	
11.3	(a)	Werden externe und interne Penetrationstests mindestens einmal im Jahr und nach sämtlichen signifikanten Infrastruktur- oder Anwendungsänderungen durchgeführt (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung)?	☐	☐	
	(b)	Werden bekannte ausnutzbare Schwachstellen korrigiert und wird anschließend ein erneuter Test durchgeführt?	☐	☐	
	(c)	Werden die Tests von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	☐	☐	
	Umfassen diese Penetrationstests folgende Punkte:				
11.3.1		Penetrationstests auf Netzwerkebene, ***Hinweis**: Die Tests müssen Komponenten enthalten, die Netzwerkfunktionen und Betriebssysteme unterstützen.*	☐	☐	
11.3.2		Penetrationstests auf Anwendungsebene. ***Hinweis**: In den Tests sollten mindestens die in der Anforderung 6.5 aufgeführten Schwachstellen überprüft werden.*	☐	☐	
11.4	(a)	Werden Systeme zur Erkennung und/oder Verhinderung von Angriffsversuchen, zur Überwachung des kompletten Datenverkehrs in der Umgebung, in der sich Karteninhaberdaten befinden, sowie kritischer Punkte innerhalb der Karteninhaberdaten-Umgebung verwendet und wird das Personal bei mutmaßlichen Sicherheitsverletzungen alarmiert?	☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	(b) Sind IDS und/oder IPS so konfiguriert, dass das Personal bei mutmaßlichen Sicherheitsverletzungen alarmiert wird?		☐	☐	
	(c) Werden Angriffserfassungs- und -vorbeugungssysteme, Standardeinstellungen und Signaturen fortwährend aktualisiert?		☐	☐	
11.5	(a) Werden in der Karteninhaberdaten-Umgebung Tools zur Überwachung der Dateiintegrität eingesetzt? Dateien, die überwacht werden sollten, sind u. a.: • Ausführbare Systemdateien, • Ausführbare Anwendungsdateien, • Konfigurations- und Parameterdateien, • Zentral gespeicherte Protokoll- und Audit-Dateien (alt oder archiviert).		☐	☐	
	(b) Sind die Tools so konfiguriert, dass das Personal über nicht autorisierte Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmiert wird, und stellen diese Tools mindestens wöchentlich Vergleiche wichtiger Dateien her? ***Hinweis**: Für die Dateiintegritätsüberwachung sind wichtige Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung aber auf eine Sicherheitsverletzung im System oder auf das Risiko einer Verletzung hinweisen könnte. Produkte zur Dateiintegritätsüberwachung sind in der Regel mit wichtigen Dateien für das jeweilige Betriebssystem vorkonfiguriert. Andere kritische Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstanbieter) beurteilt und definiert werden.*		☐	☐	

Befolgung einer Informationssicherheitsrichtlinie

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

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
12.1		Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und an das betroffene Personal weitergeleitet? *Zum Zwecke der Anforderung 12 bezieht sich der Begriff „Mitarbeiter" hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Stelle „ansässig" sind oder anderweitig Zugriff auf die Karteninhaberdaten-Umgebung haben.*	☐	☐	
	12.1.1	Umfasst die Richtlinie sämtliche PCI-DSS-Anforderungen?	☐	☐	
	12.1.2	(a) Wird der jährliche Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten in einer offiziellen Risikobeurteilung dokumentiert? (Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.)	☐	☐	
		(b) Wird der Risikobewertungsprozess mindestens einmal jährlich durchgeführt?	☐	☐	
	12.1.3	Wird die Richtlinie zur Informationssicherheit mindestens einmal im Jahr überarbeitet und an die geänderten Geschäftsziele bzw. Risiken angepasst?	☐	☐	
12.2		Werden tägliche Betriebssicherheitsverfahren entwickelt, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren) und umfassen diese administrative und technische Verfahren für jede einzelne Anforderung?	☐	☐	
12.3		Wurden Verwendungsrichtlinien für wichtige Technologien (z. B. Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, PDAs, E-Mail-Programme und Internet) entwickelt, welche allen Mitarbeitern die korrekte Verwendung dieser Technologien erläutern und folgende Punkte voraussetzen?			
	12.3.1	Ausdrückliche Genehmigung durch autorisierte Parteien, diese Technologien zu benutzen;	☐	☐	
	12.3.2	Authentifizierung zur Verwendung der Technologien;	☐	☐	
	12.3.3	Eine Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff;	☐	☐	
	12.3.4	Etikettierung von Geräten, um Eigentümer, Kontaktinformationen und Zweck zu bestimmen;	☐	☐	
	12.3.5	Akzeptable Verwendungen dieser Technologien;	☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	12.3.6	Akzeptable Netzwerkorte für die Technologien;	☐	☐	
	12.3.7	Liste der vom Unternehmen zugelassenen Produkte;	☐	☐	
	12.3.8	Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität;	☐	☐	
	12.3.9	Aktivierung von Remotezugriff-Technologien für Anbieter und Geschäftspartner nur, wenn bei Anbietern und Geschäftspartnern ein dringender Bedarf besteht und die Technologie nach der Nutzung gleich wieder deaktiviert wird.	☐	☐	
	12.3.10	(a) Falls Mitarbeiter auf Karteninhaberdaten per Remote-Zugriff zugreifen, wird in der Richtlinie untersagt, Karteninhaberdaten auf lokale Festplatten und elektronische Wechselmedien zu kopieren, zu verschieben oder zu speichern, sofern nicht ausdrücklich aufgrund bekannter Geschäftsbedürfnisse gestattet?	☐	☐	
		(b) Sieht die Richtlinie für Mitarbeiter mit entsprechenden Befugnissen den Schutz der Karteninhaberdaten gemäß den PCI-DSS-Anforderungen vor?	☐	☐	
12.4		Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	☐	☐	
12.5		Werden die Verantwortlichkeiten in Sachen Sicherheit formal einem Sicherheitsbeauftragten oder einem anderen für die Sicherheit zuständigem Mitglied des Managements übertragen?	☐	☐	
		Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?			
	12.5.1	Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren;	☐	☐	
	12.5.2	Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das jeweilige Personal;	☐	☐	
	12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?	☐	☐	
	12.5.4	Verwaltung von Benutzerkonten einschließlich Hinzufügen, Löschen und Ändern;	☐	☐	
	12.5.5	Überwachung und Kontrolle des gesamten Datenzugriffs;	☐	☐	
12.6		(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten zu vermitteln?	☐	☐	
		(b) Umfassen die Verfahren des Sicherheitsbewusstseinsprogramms folgende Punkte:			

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	12.6.1	(a) Werden im Sicherheitsbewusstseinsprogramm mehrere Methoden zur Vermittlung des Bewusstseins für Sicherheitsprobleme angesprochen (beispielsweise Poster, Briefe, Memos, webbasierte Schulungen, Meetings und Sonderaktionen)? ***Hinweis:*** *Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechte auf Karteninhaberdaten.*	☐	☐	
		(b) Werden Mitarbeiterschulungen anlässlich von Neueinstellungen und anschließend mindestens einmal im Jahr durchgeführt?	☐	☐	
	12.6.2	Werden die Mitarbeiter mindestens einmal pro Jahr aufgefordert zu bestätigen, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben?	☐	☐	
12.7		Werden potenzielle Mitarbeiter (siehe Definition des Begriffs „Personal“ unter Punkt 12.1 oben) vor der Einstellung eingehend geprüft, um das Risiko interner Angriffe so gering wie möglich zu halten? (Beispiele für Hintergrundinformationen sind frühere Tätigkeiten, eventuelle Vorstrafen, die finanzielle Situation und Referenzen bisheriger Arbeitgeber.) ***Hinweis****: Für potentielle neue Mitarbeiter wie z. B. Kassierer, die nur Zugriff auf jeweils eine Kartennummer gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.*	☐	☐	
12.8		Falls Dienstanbieter Zugriff auf Karteninhaberdaten haben, werden wie folgt Richtlinien zur Verwaltung von Dienstanbietern umgesetzt und eingehalten?			
	12.8.1	Wird eine Liste der Dienstanbieter geführt?	☐	☐	
	12.8.2	Existiert eine schriftliche Vereinbarung mit einer Bestätigung, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten in seinem Besitz haftet?	☐	☐	
	12.8.3	Gibt es ein eindeutiges Verfahren für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht?	☐	☐	
	12.8.4	Gibt es ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard?	☐	☐	
12.9		Wurde wie folgt ein Vorfallreaktionsplan implementiert, um umgehend auf mögliche Sicherheitsverletzungen im System zu reagieren?			
	12.9.1	(a) Wurde ein Vorfallreaktionsplan erstellt, der im Falle einer Systemsicherheitsverletzung im System implementiert wird?	☐	☐	
		(b) Umfasst der Plan mindestens die folgenden Punkte?			

PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	▪ Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken;	☐	☐	
	▪ Konkrete Verfahren für die Reaktion auf Vorfälle;	☐	☐	
	▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs;	☐	☐	
	▪ Verfahren zur Datensicherung;	☐	☐	
	▪ Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen;	☐	☐	
	▪ Abdeckung sämtlicher wichtigen Systemkomponenten;	☐	☐	
	▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle.	☐	☐	
12.9.2	Wird der Plan mindestens jährlich getestet?	☐	☐	
12.9.3	Steht bestimmtes Personal rund um die Uhr zur Verfügung, um auf Alarme zu reagieren?	☐	☐	
12.9.4	Werden die Mitarbeiter mit Verantwortung im Bereich der Sicherheitsverletzungs-Reaktion angemessen geschult?	☐	☐	
12.9.5	Werden in diesem Vorfallreaktionsplan Alarmmeldungen aus Intrusionserfassungs-, -vorbeugungs- und Datei-Integritätsüberwachungssystemen eingeschlossen?	☐	☐	
12.9.6	Wurde ein Prozess entwickelt und implementiert, um den Vorfallreaktionsplan je nach den gelernten Lektionen und Branchenentwicklungen zu ändern und zu aktualisieren?	☐	☐	

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

Anforderung A.1: Von mehreren Benutzern genutzte Hosting-Anbieter müssen die Karteninhaberdaten-Umgebung schützen.

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
A.1	Werden die gehostete Umgebung und die Daten jeder Stelle (d. h. Händler, Dienstanbieter oder andere Stellen) gemäß A.1.1 bis A.1.4 geschützt? *Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen.* *Hinweis: Auch wenn ein Hosting-Anbieter diese Anforderungen erfüllt, ist nicht garantiert, dass die Stelle, die den Hosting-Anbieter nutzt, die Konformitätskriterien erfüllt. Jede Stelle muss PCI-DSS-konform arbeiten und die Konformität von Fall zu Fall beurteilen.*				
A.1.1	Führen die Stellen Prozesse aus, die ausschließlich Zugriff auf die Karteninhaberdaten-Umgebung der betreffenden Stelle haben, und verwenden diese ausgeführten Anwendungsprozesse die einmalige ID der jeweiligen Stelle? Beispiel: • Keine Stelle im System kann die Benutzer-ID eines gemeinsamen Webservers verwenden. • Sämtliche von einer Stelle verwendeten CGI-Skripte müssen als eindeutige Benutzer-ID der Stelle erstellt und ausgeführt werden.		☐	☐	
A.1.2	Sind die Zugriffsberechtigungen und Rechte jeder Stelle wie folgt auf die eigene Karteninhaberdaten-Umgebung beschränkt?				
	(a) Verfügen die Benutzer-IDs eines Anwendungsprozesses tatsächlich nicht über besondere Rechte (root/admin)?		☐	☐	
	(b) Besitzen die einzelnen Stellen Lese-, Schreib- und Ausführungsberechtigungen nur für eigene Dateien und Verzeichnisse oder auch für notwendige Systemdateien (eingeschränkt durch Dateisystemberechtigungen, Zugriffssteuerungslisten, Chroot, Jailshell usw.)? *Wichtig: Die Dateien einer Stelle können nicht von einer Gruppe gemeinsam genutzt werden.*		☐	☐	
	(c) Haben tatsächlich keine Benutzer von Stellen Schreibzugriff auf gemeinsam genutzte Systemdateien erhalten?		☐	☐	

	PCI-DSS Frage	Antwort:	Ja	Nein	Spezial*
	(d) Ist die Anzeige von Protokolleinträgen auf die protokollbesitzende Stelle beschränkt?		☐	☐	
	(e) Gibt es Beschränkungen für die Nutzung folgender Systemressourcen? • Festplattenkapazität, • Bandbreite, • Arbeitsspeicher, • Prozessor. *Damit wird sichergestellt, dass einzelnen Stellen die Serverressourcen nicht komplett für sich in Anspruch nehmen können, um Anfälligkeiten auszunutzen (wie etwa Fehler-, Konkurrenz- und Neustartbedingungen, die beispielsweise zu Pufferüberläufen führen können).*		☐	☐	
A.1.3	Sind Protokollierungs- und Audit-Trails für die Karteninhaberdaten-Umgebung jeder Stelle aktiviert und eindeutig und entsprechen diese der PCI-DSS-Anforderung 10? Ist die Protokollfunktion wie folgt in allen Händler- und Dienstanbieter-Umgebungen aktiviert?		☐	☐	
	• Werden die Protokolle für gängige Anwendungen von Drittanbietern aktiviert?		☐	☐	
	• Sind die Protokolle standardmäßig aktiviert?		☐	☐	
	• Können die Protokolle von der Stelle, die sie besitzt, eingesehen werden?		☐	☐	
	• Erhalten die Besitzer der Protokolle eine Mitteilung zum genauen Speicherort der Protokolle?		☐	☐	
A.1.4	Wurden schriftliche Richtlinien und Prozesse implementiert, um eine rechtzeitige Ursachenanalyse zu ermöglichen, falls die Sicherheit bei einem gehosteten Händler oder Dienstanbieter verletzt wurde?		☐	☐	

Anhang B: Kompensationskontrollen

Kompensationskontrollen können in den meisten Fällen, in denen eine Stelle eine explizite PCI-DSS-Anforderung aufgrund von legitimen technischen oder dokumentierten geschäftlichen Einschränkungen nicht exakt erfüllen kann, in Erwägung gezogen werden. Voraussetzung hierfür ist jedoch, dass der mit der Nichterfüllung verbundene Risikozuwachs durch die Implementierung von Kontrollen an anderer Stelle kompensiert wird.

Kompensationskontrollen müssen die folgenden Kriterien erfüllen:

1. Sie müssen in Absicht und Anspruch den ursprünglichen PCI-DSS-Anforderungen entsprechen.
2. Sie müssen ein vergleichbares Schutzniveau wie die ursprüngliche PCI-DSS-Anforderung bieten. Dies bedeutet, dass die Kompensationskontrolle die Risiken, gegen die die ursprüngliche PCI-DSS-Anforderung gerichtet war, in ausreichendem Maße verhindert. (Der Zweck der einzelnen PCI-DSS-Anforderungen ist unter *PCI-DSS-Navigation erläutert.)*
3. Sie müssen mindestens so weitreichend wie andere PCI-DSS-Anforderungen sein. (Die reine Konformität mit anderen PCI-DSS-Anforderungen reicht als Kompensation nicht aus.)

   Beachten Sie folgende Anhaltspunkte für die Definition von „mindestens so weitreichend“:

   Hinweis: Die Punkte a) bis c) sind nur als Beispiel gedacht. Sämtliche Kompensationskontrollen müssen vom Prüfer, der auch die PCI-DSS-Prüfung vornimmt, daraufhin geprüft werden, ob sie eine ausreichende Kompensation darstellen. Die Effektivität einer Kompensationskontrolle hängt von der jeweiligen Umgebung ab, in der die Kontrolle implementiert wird, von den umgebenden Sicherheitskontrollen und der Konfiguration der Kontrolle. Den Unternehmen muss bewusst sein, dass eine bestimmte Kompensationskontrolle nicht in allen Umgebungen effektiv ist.

   a) Vorhandene PCI-DSS-Anforderungen können NICHT als Kompensationskontrollen betrachtet werden, wenn sie für das in Frage kommende Element ohnehin erforderlich sind. Zum Beispiel müssen Kennwörter für den nicht über die Konsole vorgenommenen Administratorzugriff verschlüsselt versendet werden, damit Administratorkennwörter nicht von Unbefugten abgefangen werden können. Als Kompensation für eine fehlende Kennwortverschlüsselung können nicht andere PCI-DSS-Kennwortanforderungen wie das Aussperren von Eindringlingen, die Einrichtung komplexer Kennwörter usw. ins Feld geführt werden, da sich mit diesen Anforderungen das Risiko eines Abfangens unverschlüsselter Kennwörter nicht reduzieren lässt. Außerdem sind die anderen Kennwortkontrollen bereits Bestandteil der PCI-DSS-Anforderungen für das betreffende Element (Kennwort).

   b) Vorhandene PCI-DSS-Anforderungen können EVENTUELL als Kompensationskontrollen betrachtet werden, wenn sie zwar für einen anderen Bereich, nicht aber für das in Frage kommende Element erforderlich sind. Beispiel: Beim Remote-Zugriff ist nach PCI-DSS eine Authentifizierung anhand zweier Faktoren erforderlich. Die Authentifizierung anhand zweier Faktoren *innerhalb des internen Netzwerks* kann für den nicht über die Konsole stattfindenden Administratorzugriff als Kompensationskontrolle betrachtet werden, wenn eine Übertragung verschlüsselter Kennwörter nicht möglich ist. Die Authentifizierung anhand zweier Faktoren ist eine akzeptable Kompensationskontrolle, wenn (1) die Absicht der ursprünglichen Anforderung erfüllt wird (das Risiko des Abfangens unverschlüsselter Kennwörter wird verhindert) und (2) die Authentifizierung in einer sicheren Umgebung ordnungsgemäß konfiguriert wurde.

   c) Die vorhandenen PCI-DSS-Anforderungen können mit neuen Kontrollen zusammen als Kompensationskontrolle fungieren. Beispiel: Ein Unternehmen kann Karteninhaberdaten nicht nach Anforderung 3.4 unlesbar machen (z. B. durch Verschlüsselung). In diesem Fall könnte eine Kompensation darin bestehen, dass mit einem Gerät bzw. einer Kombination aus Geräten, Anwendungen und Kontrollen folgende Punkte sichergestellt sind: (1) Interne Netzwerksegmentierung; (2) Filtern von IP- oder MAC-Adressen und (3) Authentifizierung anhand zweier Faktoren innerhalb des internen Netzwerks.

4. Sie müssen dem zusätzlichen Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht, angemessen sein.

Der Prüfer führt im Rahmen der jährlichen PCI-DSS-Beurteilung eine eingehende Überprüfung der Kompensationskontrollen durch und stellt dabei unter Beachtung der vier oben genannten Kriterien fest, ob die jeweiligen Kompensationskontrollen einen angemessenen Schutz vor den Risiken bieten, wie er mit der ursprünglichen PCI-DSS-Anforderung erzielt werden sollte. Zur Wahrung der Konformität müssen Prozesse und Kontrollen implementiert sein, mit denen die Wirksamkeit der Kompensationskontrollen auch nach Abschluss der Beurteilung gewährleistet bleibt.

Anhang C: Arbeitsblatt – Kompensationskontrollen

Mit diesem Arbeitsblatt können Sie die Kompensationskontrollen für jede Anforderung definieren, bei der „JA“ ausgewählt wurde und in der Spalte „Spezial“ Kompensationskontrollen genannt wurden.

Hinweis: *Nur Unternehmen, die eine Risikoanalyse vorgenommen haben und legitime technologische oder dokumentierte geschäftliche Hindernisse nachweisen können, können den Einsatz von Kompensationskontrollen zu Konformitätszwecken in Erwägung ziehen.*

Anforderungsnummer und -definition:

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

Kompensationskontrollen – Arbeitsblatt – Beispiel

Mit diesem Arbeitsblatt können Sie die Kompensationskontrollen für jede Anforderung definieren, bei der „JA“ ausgewählt wurde und in der Spalte „Spezial“ Kompensationskontrollen genannt wurden.

Anforderungsnummer: *8.1 – Werden alle Benutzer mit einem eindeutigen Benutzernamen identifiziert, bevor ihnen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird?*

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	*Unternehmen XYZ verwendet eigenständige Unix-Server ohne LDAP. Daher ist die Anmeldung als „root“ erforderlich. Es ist für Unternehmen XYZ nicht möglich, die Anmeldung „root“ zu verwalten und alle „root“-Aktivitäten für jeden einzelnen Benutzer zu protokollieren.*
2. Ziel	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	*Die Anforderung eindeutiger Anmeldungsinformationen verfolgt zwei Ziele. Zum einen ist es aus Sicherheitsgründen nicht akzeptabel, wenn Anmeldeinformationen gemeinsam verwendet werden. Zum anderen kann bei gemeinsamer Verwendung von Anmeldeinformationen nicht definitiv geklärt werden, ob eine bestimmte Person für eine bestimmte Aktion verantwortlich ist.*
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	*Für das Zugriffskontrollsystem entsteht ein zusätzliches Risiko, da nicht gewährleistet ist, dass alle Benutzer eine eindeutige ID haben und verfolgt werden können.*
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	*Unternehmen XYZ erfordert von allen Benutzern die Anmeldung an den Servern über ihre Desktop-Computer unter Verwendung des Befehls SU. SU ermöglicht einem Benutzer den Zugriff auf das Konto „root“ und die Durchführung von Aktionen unter dem Konto „root“, wobei der Vorgang im Verzeichnis „SU-log“ protokolliert werden kann. Auf diese Weise können die Aktionen der einzelnen Benutzer über das SU-Konto verfolgt werden.*
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	*Unternehmen XYZ demonstriert dem Prüfer die Ausführung des Befehls SU und die Tatsache, dass die Einzelpersonen, die den Befehl ausführen, mit „root“-Rechten angemeldet sind.*
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	*Unternehmen XYZ dokumentiert Prozesse und Verfahren, mit denen sichergestellt wird, dass SU-Konfigurationen nicht durch Änderung, Bearbeitung oder Löschen so bearbeitet werden können, dass eine*

		Ausführung von „root“-Befehlen ohne individuelle Benutzerverfolgung bzw. Protokollierung möglich würde.

Anhang D: Erläuterung der Nichtanwendbarkeit

Falls in der Spalte „Spezial“ „N/A“ oder „Nicht anwendbar“ eingegeben wurde, erläutern Sie bitte im Arbeitsblatt, warum die zugehörige Anforderung nicht für Ihr Unternehmen gilt.

Anforderung	Grund, warum die Anforderung nicht anwendbar ist.
Beispiel: *9.3.1*	*Besuchern ist es nicht gestattet, Bereiche zu betreten, an denen Karteninhaberdaten verarbeitet oder gepflegt werden.*