



Payment Card Industry (PCI)
Datensicherheitsstandard
Selbstbeurteilungs-Fragebogen D
und Compliance-Bescheinigung

**Alle anderen Händler und alle für den SBF
qualifizierten Dienstleister**

Version 1.2

Oktober 2008

Dokumentänderungen

Datum	Version	Beschreibung
1. Oktober 2008	1.2	Angeleichen von Inhalten an den neuen PCI-DSS v1.2 und Implementieren kleinerer Änderungen an der Ursprungsversion v1.1.

Inhalt

Dokumentänderungen	i
PCI-Datensicherheitsstandard: Damit verbundene Dokumente	iii
Vorbereitung.....	iv
Ausfüllen des Selbstbeurteilungs-Fragebogens	iv
PCI DSS-Konformität – Schritte zum Ausfüllen.....	iv
Anweisungen zur Nichtanwendbarkeit und zum bestimmter Anforderungen.....	v
Compliance-Bescheinigung, SBF D — Version für Händler.....	1
Compliance-Bescheinigung, SBF D — Version für Dienstanbieter	4
Selbstbeurteilungs-Fragebogen D.....	7
Erstellung und Wartung eines sicheren Netzwerks	7
<i>Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten.....</i>	<i>7</i>
<i>Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden</i>	<i>9</i>
Schutz von Karteninhaberdaten	11
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten.....</i>	<i>11</i>
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze.....</i>	<i>13</i>
Wartung eines Anfälligkeits-Managementprogramms.....	15
<i>Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware.....</i>	<i>15</i>
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen</i>	<i>15</i>
Implementierung starker Zugriffskontrollmaßnahmen	18
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf.....</i>	<i>18</i>
<i>Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff.....</i>	<i>19</i>
<i>Anforderung 9: Beschränkung des physischen Zugriff auf Karteninhaberdaten</i>	<i>20</i>
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken.....	23
<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten.....</i>	<i>23</i>
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse</i>	<i>24</i>
Befolgung einer Informationssicherheits-Richtlinie	26
<i>Anforderung 12: Richtlinie aufrecht erhalten, die Informationssicherheit für Mitarbeiter und Subunternehmer anspricht</i>	<i>26</i>
Anhang A: Zusätzliche PCI DSS-Anforderungen für Anbieter von gemeinsamem Hosting	29
<i>Anforderung A.1: Gemeinsam beauftragte Hosting-Anbieter müssen Karteninhaberdaten-Umgebung schützen</i>	<i>29</i>
Anhang B: Kompensationskontrollen	30
Anhang C: Arbeitsblatt zu Kompensationskontrollen	32
Arbeitsblatt zu Kompensationskontrollen — Muster	33
Anhang D: Erläuterung der Nichtanwendbarkeit	34

PCI-Datensicherheitsstandard: Damit verbundene Dokumente

Die folgenden Dokumente wurden als Hilfe für Händler und Dienstleister entwickelt, damit sie besser über den PCI-Datensicherheitsstandard (DSS) und den PCI DSS-SBF informiert werden.

Dokument	Publikum
<i>PCI-Datensicherheitsstandard – Anforderungen und Sicherheitsbeurteilungsverfahren</i>	Alle Händler und Dienstleister
<i>PCI DSS-Navigation: Verständnis der Intention der Anforderungen</i>	Alle Händler und Dienstleister
<i>PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung</i>	Alle Händler und Dienstleister
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen A und Bescheinigung</i>	Händler ¹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen B und Bescheinigung</i>	Händler ¹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen C und Bescheinigung</i>	Händler ¹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen D und Bescheinigung</i>	Händler ¹ und alle Dienstleister
<i>PCI-DSS- und PCI-PA-Glossar für Begriffe, Abkürzungen und Akronyme (PCI Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms)</i>	Alle Händler und Dienstleister

¹ Informationen zum Bestimmen des angemessenen Selbstbeurteilungs-Fragebogens 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 Selbstbeurteilungs-Fragebogens

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

SBF-Validierung styp	Beschreibung	SBF
1	Händler, bei denen Karte nicht vorliegt (E-Commerce oder Bestellung per Post/Telefon), alle Karteninhaber-Datenfunktionen extern vergeben. <i>Dies würde für Händler mit physischer Präsenz nie gelten.</i>	A
2	Nur-Abdruck-Händler ohne elektronischen Karteninhaber-Datenspeicher	B
3	Händler mit eigenständigen Terminals, kein elektronischer Karteninhaber-Datenspeicher	B
4	Händler mit POS-Systemen, die mit dem Internet verbunden sind, kein elektronischer Karteninhaber-Datenspeicher	C
5	Alle anderen Händler (nicht in den Beschreibungen für SBF A-C oben enthalten) und alle Dienstanbieter, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden.	D

Händler, die die Kriterien für die SBF A-C oben nicht erfüllen, und alle Dienstanbieter, die durch eine Zahlungsmarke als für den SBF qualifiziert definiert werden, werden hier und im Dokument *Anleitung und Richtlinien zum PCI DSS Selbstbeurteilungs-Fragebogen* Validierungstyp 5 zugeordnet.

Während viele Unternehmen, die SBF D ausfüllen, die Compliance mit jeder PCI DSS-Anforderung 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 Compliance mit den Abschnitten des PCI DSS, die sich speziell auf drahtlose Technologie 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-Datensicherheitsstandard.

PCI DSS-Konformität – Schritte zum Ausfüllen

1. Füllen Sie den Selbstbeurteilungs-Fragebogen (SBF D) gemäß den Anweisungen unter *Anleitung und Richtlinien zum Selbstbeurteilungs-Fragebogen* aus.
2. Führen Sie einen bestandenen Anfälligkeitsscan mit einem von PCI SSC zugelassenen Scanninganbieter (Approved Scanning Vendor oder ASV) durch und lassen Sie sich einen bestandenen Scan vom ASV nachweisen.
3. Füllen Sie die Compliance-Bescheinigung komplett aus.
4. Reichen Sie den SBF, den Nachweis eines bestandenen Scans und die Compliance-Bescheinigung zusammen mit allen anderen erforderlichen Dokumenten bei Ihrem Acquirer (Händler) oder bei der Zahlungsmarke oder einer anderen Anforderungsstelle (Dienstanbieter) ein.

Anweisungen zur Nichtanwendbarkeit und zum bestimmter Anforderungen

Ausschluss: Wenn Sie SBF D ausfüllen müssen, um Ihre PCI DSS-Compliance zu bestätigen, können folgende Ausnahmen berücksichtigt werden: Siehe „Nichtanwendbarkeit“ für die entsprechende SFB-Antwort.

- Die spezifischen Fragen zur Wireless-Technologie müssen nur beantwortet werden, wenn Wireless-Technologie in Ihrem Netzwerk verwendet wird (z. B. Anforderungen 1.2.3, 2.1.1 und 4.1.1). Bitte beachten Sie, dass Anforderung 11.1 (Verwendung eines Analysators für drahtlose Netzwerke) auch beantwortet werden muss, wenn Sie in Ihrem Netzwerk keine drahtlose Technologie verwenden, weil der Analysator alle sicherheitsgefährdenden oder nicht berechtigten Geräte erfasst, die vielleicht ohne das Wissen des Händlers hinzugefügt wurden.
- Die Fragen zu benutzerdefinierten Anwendungen und Codes (Anforderungen 6.3-6.5) müssen nur beantwortet werden, wenn Ihr Unternehmen eigene benutzerdefinierte Webanwendungen programmiert.
- Die Fragen zu den Anforderungen 9.1-9.4 müssen nur für Einrichtungen mit „Zugangsbeschränkten Bereichen“ (nachfolgend 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. Nicht hierzu zählen die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassensbereich im Einzelhandel).

Nichtanwendbarkeit: Diese und alle anderen Anforderungen, die als nicht anwendbar für Ihre Umgebung gelten, müssen durch den Vermerk „Nicht zutr.“ in der Spalte „Spezial“ des SBF gekennzeichnet sein. Füllen Sie das Arbeitsblatt „Erläuterung der Nichtanwendbarkeit“ im Anhang für jeden „Nicht zutr.“-Eintrag dementsprechend aus.

Compliance-Bescheinigung, SBF D — Version für Händler

Anleitung zum Einreichen

Der Händler muss diese Compliance-Bescheinigung einreichen, um zu bestätigen, dass er den Compliance-Status mit den *PCI-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren* erfüllt. Füllen Sie alle zutreffenden Abschnitte aus und schlagen Sie die Anleitung zum Einreichen unter „PCI DSS-Compliance – Schritte zum Ausfüllen“ in diesem Dokument nach.

Teil 1. Informationen des qualifizierten Sicherheitsprüfers (falls vorhanden)

Name des Unternehmens:					
QSA-Leiter:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2. Informationen zum Händlerunternehmen

Name des Unternehmens:		DBA(S):			
Name des Ansprechpartners:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

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

- Einzelhändler
 Telekommunikation
 Lebensmittel und Supermärkte
 Erdöl/Erdgas
 E-Commerce
 Post-/Telefonbestellung
 Sonstiges (bitte angeben):

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

Teil 2b. Beziehungen

Hat Ihr Unternehmen eine Beziehung mit einem oder mehreren Drittdienstleistern (z. B. Gateways, Webhosting-Unternehmen, Buchungspersonal von Fluggesellschaften, Vertreter von Kundentreueprogrammen usw.)?

Ja Nein

Hat Ihr Unternehmen eine Beziehung zu mehr als einem Acquirer? Ja Nein

Teil 2c. Transaktionsverarbeitung

Verwendete Zahlungsanwendung: _____ Version der Zahlungsanwendung: _____

Teil 3. PCI DSS-Validierung

Anhand der Ergebnisse, die in SBF D mit Datum vom (*completion date*) notiert wurden, bestätigt (*Merchant Company Name*) folgenden Compliance-Status (eine Option auswählen):

- Konform:** Alle Abschnitte des PCI SBF sind komplett und alle Fragen wurden mit „Ja“ beantwortet, was zu der Gesamtbewertung **VOLLE COMPLIANCE** geführt hat, **und** ein Scan wurde von einem von PCI SSC zugelassenen Scananbieter durchgeführt und bestanden, wodurch (*Merchant Company Name*) die volle Compliance mit dem PCI DSS demonstriert hat.
- Nicht konform:** Nicht alle Abschnitte des PCI DSS-SBF sind komplett oder einige Fragen wurden nicht mit „Ja“ beantwortet, was zu der Gesamtbewertung **KEINE COMPLIANCE** geführt hat, **oder** es wurde kein Scan von einem von PCI SSC zugelassenen Scananbieter durchgeführt und bestanden, wodurch (*Merchant Company Name*) nicht die volle Compliance mit dem PCI DSS demonstriert 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“

Händler bestätigt:

- PCI DSS Selbstbeurteilungs-Fragebogen D, Version (*version of SAQ*), 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 bestätige, dass ich jederzeit meine volle PCI DSS-Compliance haben muss.
- Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifendaten (aus einer Spur)², CAV2-, CVC2-, CID-, CVV2-Daten³ oder PIN-Daten⁴ gespeichert wurden.

Teil 3b. Bestätigung durch Händler

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

Vertretenes Händlerunternehmen ↑

² Im Magnetstreifen verschlüsselte Daten, 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 Verfolgungsdaten, 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.

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

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen „Compliance-Status“ für jede Anforderung aus. Wenn Sie eine der Anforderungen mit „NEIN“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung erfüllt. 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	Compliance-Status (eine Option auswählen)		Abhilfedatum und Aktionen (bei Compliance- Status „Keine Compliance“)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	<input type="checkbox"/>	<input type="checkbox"/>	
3	Schutz gespeicherter Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	<input type="checkbox"/>	<input type="checkbox"/>	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	<input type="checkbox"/>	<input type="checkbox"/>	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	<input type="checkbox"/>	<input type="checkbox"/>	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	<input type="checkbox"/>	<input type="checkbox"/>	
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	<input type="checkbox"/>	<input type="checkbox"/>	
9	Beschränkung des physischen Zugriff auf Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	<input type="checkbox"/>	<input type="checkbox"/>	
12	Befolgung einer Informationssicherheits-Richtlinie	<input type="checkbox"/>	<input type="checkbox"/>	

Compliance-Bescheinigung, SBF D — Version für Dienstanbieter

Anleitung zum Einreichen

Der Dienstanbieter muss diese Compliance-Bescheinigung einreichen, um zu bestätigen, dass er den Compliance-Status mit den *PCI-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren* erfüllt. Füllen Sie alle zutreffenden Abschnitte aus und schlagen Sie die Anleitung zum Einreichen unter „PCI DSS-Compliance – Schritte zum Ausfüllen“ in diesem Dokument nach.

Teil 1. Informationen des qualifizierten Sicherheitsprüfers (falls vorhanden)

Name des Unternehmens:					
QSA-Leiter:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2. Informationen zum Dienstanbieterunternehmen

Name des Unternehmens:					
Name des Ansprechpartners:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2a. Dienste

Angebote Dienste (alle zutreffenden auswählen):

- | | | |
|--|--|---|
| <input type="checkbox"/> Autorisierung | <input type="checkbox"/> Treueprogramme | <input type="checkbox"/> 3-D Secure-Zugriffskontrollserver |
| <input type="checkbox"/> Umtausch
Magnetstreifentransaktionen | <input type="checkbox"/> IPSP (E-Commerce) | <input type="checkbox"/> Verarbeitung von |
| <input type="checkbox"/> Zahlungs-Gateway | <input type="checkbox"/> Abwicklung und Abrechnung | <input type="checkbox"/> Verarbeitung von MO/TO-Transaktionen |
| <input type="checkbox"/> Hosting | <input type="checkbox"/> Problembearbeitung | <input type="checkbox"/> Sonstiges (bitte angeben): |

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

Teil 2b. Beziehungen

Hat Ihr Unternehmen eine Beziehung mit einem oder mehreren Drittdienstanbietern (z. B. Gateways, Webhosting-Unternehmen, Buchungspersonal von Fluggesellschaften, Vertreter von Kundentreueprogrammen usw.)?

Ja Nein

Teil 2c: Transaktionsverarbeitung

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

Als Teil Ihres Dienstes verwendete oder bereitgestellte Zahlungsanwendungen:

Version der Zahlungsanwendung:

Teil 3. PCI DSS-Validierung

Anhand der Ergebnisse, die in SBF D mit Datum vom (*completion date of SAQ*) notiert wurden, bestätigt (*Service Provider Company Name*) folgenden Compliance-Status (eine Option auswählen):

- Konform:** Alle Abschnitte des PCI SBF sind komplett und alle Fragen wurden mit „Ja“ beantwortet, was zu der Gesamtbewertung **VOLLE COMPLIANCE** geführt hat, **und** ein Scan wurde von einem von PCI SSC zugelassenen Scananbieter durchgeführt und bestanden, wodurch (*Service Provider Company Name*) die volle Compliance mit dem PCI DSS demonstriert hat.
- Nicht konform:** Nicht alle Abschnitte des PCI SBF sind komplett oder einige Fragen wurden mit „Nein“ beantwortet, was zu der Gesamtbewertung **KEINE COMPLIANCE** geführt hat, **oder** es wurde kein Scan von einem von PCI SSC zugelassenen Scananbieter durchgeführt und bestanden, wodurch (*Service Provider Company Name*) nicht die volle Compliance mit dem PCI DSS demonstriert 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“

Diensteanbieter bestätigt:

- Selbstbeurteilungs-Fragebogen D, Version (*insert version number*), 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 bestätige, dass ich jederzeit meine volle PCI DSS-Compliance haben muss.
- Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifendaten (aus einer Spur)⁵, CAV2-, CVC2-, CID-, CVV2-Daten⁶ oder PIN-Daten⁷ gespeichert wurden.

Teil 3b. Bestätigung durch den Diensteanbieter

<i>Unterschrift des Beauftragten des Diensteanbieters</i> ↑	<i>Datum</i> ↑
<i>Name des Beauftragten des Diensteanbieters</i> ↑	<i>Titel</i> ↑

Vertretenes Diensteanbieterunternehmen ↑

⁵ Im Magnetstreifen verschlüsselte Daten, 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 Verfolgungsdaten, 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.

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen „Compliance-Status“ für jede Anforderung aus. Wenn Sie eine der Anforderungen mit „NEIN“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung erfüllt. 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	Compliance-Status (eine Option auswählen)		Abhilfedatum und Aktionen (bei Compliance- Status „Keine Compliance“)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	<input type="checkbox"/>	<input type="checkbox"/>	
3	Schutz gespeicherter Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	<input type="checkbox"/>	<input type="checkbox"/>	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	<input type="checkbox"/>	<input type="checkbox"/>	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	<input type="checkbox"/>	<input type="checkbox"/>	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	<input type="checkbox"/>	<input type="checkbox"/>	
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	<input type="checkbox"/>	<input type="checkbox"/>	
9	Beschränkung des physischen Zugriff auf Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	<input type="checkbox"/>	<input type="checkbox"/>	
12	Befolgung einer Informationssicherheits-Richtlinie	<input type="checkbox"/>	<input type="checkbox"/>	

Selbstbeurteilungs-Fragebogen D

Ausfülldatum:

Erstellung und Wartung eines sicheren Netzwerks

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

Frage	Antwort:	Ja	Nein	Spezial*
1.1	Umfassen die festgelegten Firewall- und Router-Konfigurationsstandards Folgendes:			
1.1.1	Einen offiziellen Prozess zur Genehmigung und zum Testen aller externen Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	Aktuelle Netzwerkdiagramme mit allen Verbindungen mit Karteninhaberdaten, einschließlich aller drahtlosen Netzwerke?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	Dokumentation und Begründung für den Einsatz aller zulässigen Dienste, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	Anforderung zum Prüfen von Firewall- und Router-Regelsätzen mindestens alle sechs Monate?	<input type="checkbox"/>	<input type="checkbox"/>	
1.2	Beschränkt die Firewall-Konfiguration die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemen in der Karteninhaberdaten-Umgebung auf die folgende Weise: <i>Hinweis: Ein „nicht vertrauenswürdige Netzwerk“ ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.</i>			
1.2.1.	Wird der ein- und ausgehende Netzwerkverkehr auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Verkehr beschränkt?	<input type="checkbox"/>	<input type="checkbox"/>	
1.2.2	Werden Router-Konfigurationsdateien gesichert und synchronisiert?	<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Sind Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung implementiert, und sind die Firewalls so konfiguriert, sodass der gesamte Verkehr aus der drahtlosen Umgebung abgelehnt oder kontrolliert wird (sofern dieser Verkehr für Geschäftszwecke notwendig ist)?	<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

Frage		Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
1.3	Verbietet die Firewall-Konfiguration den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung?				
1.3.1	Ist eine DMZ implementiert, um ein- und ausgehenden Verkehr auf Protokolle zu beschränken, die für die Karteninhaberdaten-Umgebung erforderlich sind?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	Ist der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	Sind direkte eingehenden oder ausgehenden Routen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zugelassen?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	Ist zugelassen, dass interne Adressen aus dem Internet in die DMZ übergeben werden?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	Wird der ausgehende Datenverkehr aus der Karteninhaberdaten-Umgebung in das Internet beschränkt, sodass der ausgehende Verkehr nur auf IP-Adressen innerhalb der DMZ zugreifen kann?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	Ist eine statusbehaftete Inspektion implementiert, was auch als Dynamic Packet Filtering bezeichnet wird (d. h. nur etablierte Verbindungen können in das Netzwerk gelangen)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.7	Ist die Datenbank in einer internen Netzwerkzone, die von der DMZ getrennt ist, platziert?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	Wurde die IP-Maskierung unter Verwendung des RFC 1918-Adressraums implementiert, um zu verhindern, dass interne Adressen übersetzt und im Internet offengelegt werden können? <i>Verwenden von NAT-Technologien (Network Address Translation), z. B. Port Address Translation (PAT)</i>		<input type="checkbox"/>	<input type="checkbox"/>	
1.4	Wurde eine persönliche Firewallsoftware auf allen mobilen und/oder Mitarbeitern gehörenden Computern mit direkter Verbindung mit dem Internet (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden, installiert?		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

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

	Frage	Antwort:	Ja	Nein	Spezial*
2.1	Werden vom Anbieter gelieferte Standardeinstellungen stets geändert, bevor ein System im Netzwerk installiert wird? <i>Beispiele: Kennwörter, Simple Network Management Protocol (SNMP)-Community-Zeichenfolgen und Beseitigung nicht benötigter Accounts.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	(a) Werden die Standardeinstellungen** von drahtlosen Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder Karteninhaberdaten übertragen, geändert, bevor ein drahtloses System installiert wird? <i>**Derartige Standardeinstellungen für drahtlose Umgebungen umfassen u. a. standardmäßige drahtlose Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sind die Sicherheitseinstellungen bei drahtlosen Geräten für eine starke Verschlüsselungstechnologie zur Authentifizierung und Übertragung aktiviert?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Wurden für alle Systemkomponenten Konfigurationsstandards entwickelt?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sprechen diese Standards alle bekannten Sicherheitsanfälligkeiten an und entsprechen sie in der Industrie akzeptierten Systemhärtungsstandards wie z. B. SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST) und Center for Internet Security (CIS)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Gewährleisten die Kontrollen Folgendes:				
2.2.1	Ist nur eine primäre Funktion pro Server implementiert?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	Werden alle unnötigen und unsicheren Dienste und Protokolle deaktiviert (nicht direkt für die Ausführung der spezifischen Gerätefunktion erforderliche Funktionen)?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	Werden Systemsicherheitsparameter konfiguriert, um Missbrauch zu verhindern?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	Wurden alle unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver entfernt?		<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Ist der gesamte Nichtkonsolen-Verwaltungszugriff verschlüsselt? <i>Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff</i>		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

	Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
2.4	Falls Sie ein gemeinsam genutzter Hosting-Anbieter sind, sind Ihre Systeme so konfiguriert, dass die gehostete Umgebung und die Karteninhaberdaten jeder Stelle geschützt werden? <i>Siehe Anhang A: Weitere PCI DSS-Anforderungen für gemeinsam genutzte Hosting-Anbieter“. Dort finden Sie die spezifisch zu erfüllenden Anforderungen.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

	Frage	Antwort:	Ja	Nein	Spezial*
3.1	(a) Wird die Speicherung von Karteninhaberdaten minimiert, und ist die Speichermenge und die Beibehaltungszeit auf die zu geschäftlichen, juristischen oder auflagenbedingten Zwecke notwendigen Werte beschränkt?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Gibt es eine Richtlinie zur Beibehaltung und zum Löschen von Daten und umfasst diese Beschränkungen, wie in (a) oben angegeben?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2	Halten alle Systeme die folgenden Anforderungen hinsichtlich des Speicherns vertraulicher Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind) ein?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>Nicht den gesamten Inhalt einer Spur auf dem Magnetstreifen (auf der Kartenrückseite, auf einem Chip oder an anderer Stelle) speichern. Diese Daten werden auch als Full Track, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet.</p> <p><i>Hinweis: Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:</i></p> <ul style="list-style-type: none"> ▪ Name des Karteninhabers ▪ Primary Account Number (PAN), ▪ Ablaufdatum und ▪ Servicecode <p><i>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente. Speichern Sie NIE den Kartenverifizierungscode oder -wert oder die PIN-Verifizierungswert-Datenelemente.</i></p> <p><i>Hinweis: Weitere Informationen finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>Speichern Sie nicht den Kartvalidierungscode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte), der zur Verifizierung bei Transaktionen verwendet wird, bei denen die Karte nicht physisch vorliegt.</p> <p><i>Hinweis: Weitere Informationen finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blocks speichern.		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

	Frage	Antwort:	Ja	Nein	Spezial*
3.3	<p>Ist die PAN bei der Anzeige maskiert (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden)?</p> <p><i>Hinweise:</i></p> <ul style="list-style-type: none"> ▪ Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die aus bestimmten Gründen die vollständige PAN einsehen müssen. ▪ Diese Anforderung ersetzt nicht strengere Anforderungen für die Anzeige von Karteninhaberdaten – z. B. für POS-Belege. 		<input type="checkbox"/>	<input type="checkbox"/>	
3.4	<p>Ist die PAN mindestens überall dort unter Verwendung der folgenden Verfahren unleserlich gemacht, wo sie gespeichert wird (auch auf tragbaren digitalen Medien, Sicherungsmedien und in Protokollen)?</p> <ul style="list-style-type: none"> ▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren ▪ Abkürzung ▪ Index-Token und -Pads (Pads müssen sicher aufbewahrt werden) ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und –verfahren. <p><i>Unter den Kontoinformationen MUSS MINDESTENS die PAN unleserlich gemacht werden.</i></p> <p><i>Informationen für den Fall, dass ein Unternehmen die PAN aus irgendeinem Grund nicht unleserlich machen kann, finden Sie „Anhang B: Kompensationskontrollen“.</i></p> <p><i>Hinweis: Eine Definition für „starke Kryptographie“ finden Sie im PCI DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	<p>Falls Datenträgerverschlüsselung (statt der Verschlüsselung auf Datei- oder Datenbankspaltenebene) verwendet wird:</p> <p>(a) Wird der logische Zugriff unabhängig von den Zugriffskontrollmechanismen des Betriebssystems verwaltet (z. B. indem keine lokalen Benutzerkontodatenbanken verwendet werden)?</p> <p>(b) Sind die Entschlüsselungsschlüssel von Benutzerkonten unabhängig?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	<p>Werden für die Verschlüsselung von Karteninhaberdaten verwendete kryptographische Schlüssel vor Offenlegung und Missbrauch geschützt?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.1	<p>Ist der Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Wächtern beschränkt?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	<p>Werden kryptographische Schlüssel sicher und an so wenigen Orten und in so wenigen Formen wie möglich aufbewahrt?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6	<p>(a) Werden alle Schlüsselverwaltungsprozesse und -verfahren für die zur Verschlüsselung von Karteninhaberdaten verwendeten kryptographischen Schlüssel voll dokumentiert und implementiert?</p> <p>(b) Umfasst dies Folgendes:</p>		<input type="checkbox"/>	<input type="checkbox"/>	

	Frage	Antwort:	Ja	Nein	Spezial*
3.6.1	Generierung starker kryptographischer Schlüssel		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Sichere Verteilung kryptographischer Schlüssel		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Sichere Aufbewahrung kryptographischer Schlüssel		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Regelmäßige Änderung der kryptographischen Schlüssel <ul style="list-style-type: none"> ▪ Wie von der jeweiligen Anwendung als notwendig erachtet und empfohlen (z. B. erneute Schlüsselvergabe), vorzugsweise automatisch ▪ Mindestens jährlich 		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Entfernung oder Austausch von alten oder vermeintlich beschädigten kryptographischen Schlüsseln		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Geteiltes Wissen und Festlegen dualer Schlüsselkontrolle		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Verhinderung des nicht autorisierten Ersatzes von kryptographischen Schlüsseln		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Wächter von kryptographischen Schlüsseln müssen ein Formular unterzeichnen, das besagt, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.		<input type="checkbox"/>	<input type="checkbox"/>	

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

	Frage	Antwort:	Ja	Nein	Spezial*
4.1	Werden eine starke Kryptographie sowie Sicherheitsprotokolle wie SSL/TLS oder IPSEC verwendet, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen? <i>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).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	Werden bewährte Branchenverfahren (z. B. IEEE 802.11i) für drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind, eingesetzt, um die starke Verschlüsselung für die Authentifizierung und Übertragung zu implementieren? <i>Hinweise:</i> <ul style="list-style-type: none"> ▪ Für neue drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 31. März 2009 zu implementieren. ▪ Für bestehende drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 30. Juni 2010 zu implementieren. 		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

	Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
4.2	Existieren Richtlinien, Verfahren und Praktiken, um das Senden unverschlüsselter PANs mittels Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat) auszuschließen?		<input type="checkbox"/>	<input type="checkbox"/>	

Wartung eines Anfälligkeits-Managementprogramms

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware

Frage	Antwort:	Ja	Nein	Spezial*
5.1	Wird auf allen Systemen, insbesondere PCs und Server, die in der Regel von bösartiger Software betroffen sein können, Antivirensoftware bereitgestellt?	<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Sind alle Antivirenprogramme in der Lage, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen?	<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Sind alle Antivirenmechanismen auf dem Laufenden, werden sie aktiv ausgeführt und sind sie in der Lage, Audit-Protokolle zu generieren?	<input type="checkbox"/>	<input type="checkbox"/>	

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Frage	Antwort:	Ja	Nein	Spezial*
6.1	(a) Wurden für alle Systemkomponenten und Softwareanwendungen die neuesten Sicherheitspatches des jeweiligen Herstellers installiert?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden wichtige Sicherheitspatches innerhalb eines Monats nach der Freigabe installiert? <i>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.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) Gibt es einen Prozess zur Identifizierung neu festgestellter Sicherheitsanfälligkeiten (z. B. Abonnieren von im Internet frei verfügbaren Alarmdiensten)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden Konfigurationsstandards gemäß PCI DSS-Anforderung 2.2 aktualisiert, um neue Sicherheitslückenprobleme anzugehen.	<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Werden Softwareanwendungen gemäß PCI DSS (z. B. sichere Authentifizierung und Protokollierung) und anhand von Best Practices der Branche entwickelt und wird während des gesamten Softwareentwicklungszyklus auf die Informationssicherheit geachtet?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Gewährleisten die Kontrollen Folgendes:			

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

Frage		Antwort:	Ja	Nein	Spezial*
6.3.1	Testen aller Sicherheitspatches und System- und Softwarekonfigurationsänderungen vor der Implementierung, einschließlich folgender Punkte:		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.1	Validierung der gesamten Eingabe (zum Verhindern von siteübergreifender Skripterstellung, Injektionsfehlern, böswilliger Dateiausführung usw.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.2	Validierung der ordnungsgemäßen Fehlerbehandlung		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.3	Validierung des sicheren kryptographischen Speichers		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.4	Validierung sicherer Mitteilungen		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.5	Validierung der ordnungsgemäßen rollenbasierten Zugriffssteuerung (RBAC)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.2	Separate Entwicklungs-, Test- und Produktionsumgebungen?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.3	Trennung der Aufgaben von Entwicklungs-, Test- und Produktionsumgebungen?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.4	Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.5	Entfernen von Testdaten und -konten, bevor Produktionssysteme aktiv werden?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.6	Entfernen benutzerdefinierter Anwendungskonten, Benutzer-IDs und Kennwörter vor der Aktivierung von Anwendungen oder deren Freigabe an Kunden?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.7	Überprüfung benutzerdefinierter Programmcodes vor der Freigabe an die Produktion oder an Kunden, um alle potenziellen Programmanfälligkeiten zu identifizieren? <i>Hinweis: Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus gemäß PCI DSS-Anforderung 6.3. Code-Prüfungen können durch qualifiziertes internes Personal ausgeführt werden. Webanwendungen unterliegen auch zusätzlichen Kontrollen, wenn sie öffentlich sind, um laufende Bedrohungen und Sicherheitslücken nach der Implementierung gemäß der Definition in der PCI DSS-Anforderung 6.6 anzugehen.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.4	(a) Werden Änderungskontrollverfahren für alle Änderungen an Systemkomponenten befolgt?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Stellen die Verfahren Folgendes sicher?				
6.4.1	Dokumentation der Auswirkungen?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Verwaltung der Abzeichnung durch die jeweiligen Parteien?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Testen der Betriebsfunktionalität?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Back-Out-Verfahren?		<input type="checkbox"/>	<input type="checkbox"/>	

Frage		Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
6.5	(a) Werden alle Webanwendungen (intern und extern und einschließlich des Webverwaltungszugriffs auf die Anwendung) anhand sicherer Codierungsrichtlinien, wie z. B. dem <i>Open Web Application Security Project Guide</i> , entwickelt?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Wird die Vorbeugung häufiger Programmieranfälligkeiten in Softwareentwicklungsprozessen berücksichtigt, einschließlich der folgenden Punkte: <i>Hinweis: Die unter 6.5.1 bis 6.5.10 aufgeführten Schwachstellen waren im OWASP-Handbuch zum Zeitpunkt der Veröffentlichung von PCI DSS v1.2 aktuell. Wenn das OWASP-Handbuch aktualisiert wird, muss jedoch die aktuelle Version für diese Anforderungen verwendet werden.</i>				
6.5.1	Siteübergreifendes Scripting (XSS)?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Injektionsfehler, insbesondere bei der SQL-Injektion? <i>LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Böswillige Dateiausführung?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Unsichere direkte Objektverweise?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Cross-Site Request Forgery (CSRF)?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	Informationslecks und unsachgemäße Fehlerbehandlung?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.7	Geknackte Authentifizierungs- und Sitzungsverwaltung?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Unsicherer kryptographischer Speicher?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Unsichere Mitteilungen?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.10	Unterlassene Einschränkung des URL-Zugriffs?		<input type="checkbox"/>	<input type="checkbox"/>	
6.6	Werden neue Bedrohungen und Schwachstellen bei öffentlichen Webanwendungen kontinuierlich angegangen und werden diese Anwendungen durch eine der folgenden Methoden geschützt? <ul style="list-style-type: none"> ▪ Prüfen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit mindestens jährlich sowie nach Änderungen oder ▪ Installieren einer Webanwendungs-Firewall vor öffentlichen Webanwendungen 		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

	Frage	Antwort:	Ja	Nein	Spezial*
7.1	(a) Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten nur auf die Personen beschränkt, die im Rahmen ihrer Arbeit darauf zugreifen müssen?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Umfassen die Zugriffsbeschränkungen Folgendes:				
7.1.1	Beschränkung von Zugriffsrechten für Benutzernamen auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogene Verpflichtungen erforderlich sind?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Die auf der Tätigkeitsklassifizierung und -funktion einzelner Mitarbeiter basierende Zuweisung von Berechtigungen?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Anforderung für ein vom Management unterzeichnetes Autorisierungsformular, das erforderliche Berechtigungen angibt?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Implementierung eines automatisierten Zugriffskontrollsystems?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	(a) Besteht für Systeme mit mehreren Benutzern ein Zugriffskontrollsystem, um den Zugriff anhand des Informationsbedarfs eines Benutzers zu beschränken, und ist dieses System auf „Alle ablehnen“ eingestellt, sofern der Zugriff nicht ausdrücklich zugelassen wird?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Umfasst dieses Zugriffskontrollsystem die folgenden Punkte?				
7.2.1	Abdeckung aller Systemkomponenten?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Standardeinstellung „Alle ablehnen“?		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

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

	Frage	Antwort:	Ja	Nein	Spezial*
8.1	Wird allen Benutzern eine eindeutige Benutzer-ID zugewiesen, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird?		<input type="checkbox"/>	<input type="checkbox"/>	
8.2	Werden neben der Zuweisung einer eindeutigen ID eine oder mehrere der folgenden Methoden eingesetzt, um alle Benutzer zu authentifizieren? <ul style="list-style-type: none"> ▪ Kennwort oder Kennsatz ▪ Authentifizierung mittels zweier Faktoren (z. B. Token-Geräte, Smartcards, biometrische Systeme oder öffentliche Schlüssel) 		<input type="checkbox"/>	<input type="checkbox"/>	
8.3	Ist eine Authentifizierung anhand zweier Faktoren beim Remote-Zugriff (Netzwerkzugriff von außerhalb des Netzwerks) von Mitarbeitern, Administratoren und Dritten eingerichtet? <i>Verwenden Sie Technologien wie Remote-Authentifizierung und Einwahldienst (RADIUS) oder Terminal Access Controller Access Control System (TACACS) mit Tokens bzw. VPN (basiert auf SSL/TLS oder IPSEC) mit individuellen Zertifikaten.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
8.4	Werden alle Kennwörter während der Übertragung und Speicherung auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung (siehe <i>PCI DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>) unleserlich gemacht?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5	Werden die entsprechenden Benutzerauthentifizierungs- und Kennwortverwaltungskontrollen für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten wie folgt verwendet?				
8.5.1	Werden Hinzufügen, Löschen und Modifizieren von Benutzer-IDs, Anmeldeinformationen und anderer Identifizierungsobjekte kontrolliert?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	Wird die Benutzeridentität überprüft, bevor Kennwörter zurückgesetzt werden?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	Werden Kennwörter für die erstmalige Systemverwendung für jeden Benutzer auf einen eindeutigen Wert gesetzt, und muss jeder Benutzer sein Kennwort sofort nach der ersten Verwendung ändern?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.4	Wird der Zugriff für alle entlassenen Benutzer sofort verweigert?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	Werden inaktive Benutzerkonten mindestens alle 90 Tage entfernt oder deaktiviert?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6	Sind von Lieferanten für die Remote-Pflege verwendete Accounts nur während der erforderlichen Zeit aktiviert?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Werden Kennwortverfahren und -richtlinien allen Benutzern mit Zugriff auf Karteninhaberdaten vermittelt?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	Sind Gruppen-, Freigabe- oder generische Konten und Kennwörter unzulässig?		<input type="checkbox"/>	<input type="checkbox"/>	

	Frage	Antwort:	Ja	Nein	Spezial*
8.5.9	Müssen Benutzerkennwörter mindestens alle 90 Tage geändert werden?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	Ist eine Mindestkennwortlänge von sieben Zeichen obligatorisch?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	Müssen Kennwörter sowohl numerische als auch alphabetische Zeichen enthalten?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	Muss eine Person ein neues Kennwort einreichen, das sich von den letzten vier Kennwörtern unterscheidet, die sie verwendet hat?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	Werden wiederholte Zugriffsversuche begrenzt, indem die Benutzer-ID nach mehr als sechs Versuchen ausgesperrt wird?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.14	Ist die Aussperrdauer auf 30 Minuten oder bis zur Reaktivierung der Benutzer-ID durch den Administrator eingestellt?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	Wenn in einer Sitzung mehr als 15 Minuten keine Eingaben mehr erfolgen, muss der Benutzer das Kennwort dann erneut eingeben und das Terminal reaktivieren?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	Erfolgt der gesamte Zugriff auf Datenbanken mit Karteninhaberdaten über eine Authentifizierung? (Dies umfasst Zugriff durch Anwendungen, Administratoren und alle anderen Benutzer.)		<input type="checkbox"/>	<input type="checkbox"/>	

Anforderung 9: Beschränkung des physischen Zugriff auf Karteninhaberdaten

	Frage	Antwort:	Ja	Nein	Spezial*
9.1	Werden angemessener Zugangskontrollen verwendet, um den physischen Zugriff auf Systeme für Karteninhaberdaten zu überwachen und zu beschränken?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) Überwachen Videokameras und andere Kontrollsysteme den Zugang zu zugangsbeschränkten Bereichen? <i>Hinweis: „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert werden. Nicht hierzu zählen die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden die Daten von den Videokameras überprüft und mit anderen Eingaben verglichen?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Werden die Daten von den Videokameras mindestens drei Monate lang aufbewahrt, außer dies wird gesetzlich anderweitig festgelegt?		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

Frage		Antwort:	Ja	Nein	Spezial*
9.1.2	Ist der physische Zugriff auf öffentlich zugängliche Netzwerkboxen beschränkt?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	Ist der physische Zugang auf Zugriffspunkte für drahtlose Netzwerke, Gateways und Handgeräte beschränkt?		<input type="checkbox"/>	<input type="checkbox"/>	
9.2	Werden Verfahren eingesetzt, damit das Personal zwischen Mitarbeitern und Besuchern unterscheiden kann, insbesondere in Bereichen, in denen Karteninhaberdaten zugänglich sind? <i>„Mitarbeiter“ bezieht sich hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und externe Mitarbeiter sowie Berater, die am Standort der jeweiligen Stelle „beheimatet“ sind. Ein „Besucher“ wird als Lieferant, Gast eines Mitarbeiters, Servicepersonal oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
9.3	Wird mit allen Besuchern wie folgt umgegangen:				
9.3.1	Autorisierung vor Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden?		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.2	Erhalten Sie ein physisches Kennzeichen (z. B. Ausweis oder Zuganggerät) mit begrenzter Gültigkeit und das die Besucher als Nichtmitarbeiter identifiziert?		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.3	Werden sie gebeten, das physische Kennzeichen zurückzugeben, bevor sie die Einrichtung verlassen oder am Datum des Gültigkeitsendes?		<input type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) Wird ein Benutzerprotokoll geführt, um die Besucheraktivität physisch überprüfen zu können?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden der Name des Besuchers, der Firmennamen und der Namen des Mitarbeiters, der dem Besucher Zugang gewährt, protokolliert?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Wird das Besucherprotokoll mindestens drei Monate lang oder wie gesetzlich vorgeschrieben aufbewahrt?		<input type="checkbox"/>	<input type="checkbox"/>	
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?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Wird die Sicherheit dieses Standorts mindestens einmal pro Jahr überprüft?		<input type="checkbox"/>	<input type="checkbox"/>	
9.6	Sind alle Papier- und elektronischen Medien, die Karteninhaberdaten enthalten, physisch sicher?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) Wird die interne oder externe Verteilung dieser Art von Medien, die Karteninhaberdaten enthalten, stets strikt kontrolliert?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Umfassen die Kontrollen Folgendes:				
9.7.1	Werden die Medien klassifiziert, sodass sie als vertraulich identifiziert werden können?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Werden die Medien, die per sicheren Kurier oder andere Liefermethoden gesendet werden, präzise verfolgt?		<input type="checkbox"/>	<input type="checkbox"/>	

	Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
9.8	Gibt es Prozesse und Verfahren zur Gewährleistung, dass vor dem Verlagern aller Medien mit Karteninhaberdaten aus einem gesicherten Bereich die Genehmigung durch das Management eingeholt werden muss (insbesondere wenn Medien an Einzelpersonen verteilt werden)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9	Wird die strikte Kontrolle über den Aufbewahrungsort und Zugriff auf Medien, die Karteninhaberdaten enthalten, stets bewahrt?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9.1	(a) Werden Medieninventurlisten ordnungsgemäß verwaltet?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden Medieninventuren mindestens einmal im Jahr durchgeführt?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10	Werden Medien, die Karteninhaberdaten enthalten, zerstört, wenn sie nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden? Die Zerstörung hat wie folgt zu erfolgen:		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1	Werden Daten auf festen Materialien per Shredder, durch Verbrennen oder Zerstampfen vernichtet, sodass Karteninhaberdaten nicht wiederhergestellt werden können?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Werden Karteninhaberdaten auf elektronischen Medien in einer Art und Weise gelöscht, die eine Wiederherstellung der Daten unmöglich macht?		<input type="checkbox"/>	<input type="checkbox"/>	

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

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

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?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2	Werden automatisierte Audit-Trails für alle Systemkomponenten implementiert, um folgende Ereignisse rekonstruieren zu können:				
10.2.1	Alle individuellen Benutzerzugriffe auf Karteninhaberdaten?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.2	Alle von einer Einzelperson mit root- oder Administratorrechten vorgenommene Aktionen?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.3	Zugriff auf alle Audit-Trails?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Ungültige logische Zugriffsversuche?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Verwendung von Identifizierungs- und Authentifizierungsmechanismen?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.6	Initialisierung der Audit-Protokolle?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.7	Erstellung und Löschen von Objekten auf Systemebene?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3	Werden die folgenden Audit-Trail-Einträge für alle Systemkomponenten für jedes Ereignis aufgezeichnet:				
10.3.1	Benutzeridentifizierung?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Ereignistyp?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Datum und Uhrzeit?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Erfolg oder Fehler?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Ereignisursprung?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen?		<input type="checkbox"/>	<input type="checkbox"/>	
10.4	Sind alle kritischen Systemuhren und -zeiten synchronisiert?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) Werden Audit-Trails gesichert, sodass sie nicht geändert werden können?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Gewährleisten die Kontrollen Folgendes:				
10.5.1	Ist die Anzeige der Audit-Trails auf Personen mit arbeitsbedingtem Bedarf beschränkt?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.2	Werden Audit-Trail-Dateien vor nicht autorisierten Modifizierungen geschützt?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.3	Werden Audit-Trail-Dateien prompt auf einem zentralisierten Protokollserver oder auf Medien gesichert die schwierig zu ändern sind?		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

	Frage	Antwort:	Ja	Nein	Spezial*
10.5.4	Werden Protokolle für nach außen gerichtete Technologien auf einem Protokollserver im internen LAN erstellt?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	Werden Datei-Integritätsüberwachungs- und Änderungserfassungssoftware für die Protokolle 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)?		<input type="checkbox"/>	<input type="checkbox"/>	
10.6	Werden Protokolle für alle Systemkomponenten mindestens täglich überprüft? <i>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 Compliance mit Anforderung 10.6 zu erzielen, können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	Werden Prüfprotokoll-Verlaufsdaten für den Zeitraum mindestens eines Jahres aufbewahrt, wobei ein mindestens dreimonatiger Zeitraum sofort für die Analyse bereitstehen muss (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar)?		<input type="checkbox"/>	<input type="checkbox"/>	

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

	Frage	Antwort:	Ja	Nein	Spezial*
11.1	Finden regelmäßige, mindestens einmal im Quartal erfolgende Tests auf WLAN-Zugriffspunkte mit einem Analysegerät statt oder wird ein Wireless IDS/IPS-System zur Ermittlung aller im Betrieb befindlichen drahtlosen Geräte eingesetzt?		<input type="checkbox"/>	<input type="checkbox"/>	
11.2	Werden interne und externe Netzwerkanfälligkeitsscans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Modifizierungen von Firewall-Regeln, Produktupgrades) ausgeführt? <i>Hinweis: Vierteljährliche externe Netzwerkanfälligkeitsscans müssen von einem Approved Scanning Vendor (ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI SSC) zugelassen wurde. Nach Netzwerkänderungen durchgeführte Scans können vom internen Personal des Unternehmens ausgeführt werden.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
11.3	(a) Werden mindestens einmal im Jahr und nach jeder signifikanten Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, Teilnetzwerk oder Webserver zur Umgebung hinzugefügt) externe und interne Penetrationstests durchgeführt? (b) Umfassen diese Penetrationstests Folgendes:		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

	Frage	Antwort:	Ja	Nein	Spezial*
11.3.1	Penetrationstests auf Netzwerkebene?		<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Penetrationstests auf Anwendungsebene?		<input type="checkbox"/>	<input type="checkbox"/>	
11.4	(a) Werden Systeme zur Erkennung und/oder Verhinderung von Eindringversuchen zur Überwachung des kompletten Datenverkehrs in der Umgebung, in der sich Karteninhaberdaten befinden, und zur Alarmierung des Personals bei mutmaßlichen Sicherheitsverletzungen, eingesetzt?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden alle Intrusionserfassungs- und Vorbeugungs-Engines ständig aktualisiert?		<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) Wird Datei-Integritätsüberwachungssoftware eingesetzt, um Personal über die nicht autorisierte Änderung wichtiger System-, Konfigurations- oder Inhaltsdateien zu alarmieren?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Ist die Software so konfiguriert, dass mindestens wöchentlich Vergleiche wichtiger Dateien ausgeführt werden? <i>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 das Risiko einer Verletzung hinweisen könnte. Produkte zur Dateiintegritätsüberwachung sind in der Regel mit wichtigen Dateien für das jeweilige Betriebssystem vorkonfiguriert. Andere wichtige Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstleister) beurteilt und definiert werden.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

Befolgung einer Informationssicherheits-Richtlinie

Anforderung 12: *Richtlinie aufrecht erhalten, die Informationssicherheit für Mitarbeiter und Subunternehmer anspricht*

	Frage	Antwort:	Ja	Nein	Spezial*
12.1	Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und verbreitet und hat sie Folgendes erreicht:		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.1	Umfasst sie sämtliche PCI DSS-Anforderungen?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	Umfasst sie einen jährlichen Prozess zur Identifizierung von Bedrohungen und Anfälligkeiten, der zu einer offiziellen Risikobeurteilung führt?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Umfasst sie eine Überprüfung mindestens einmal im Jahr und Aktualisierungen bei Umgebungsänderungen?		<input type="checkbox"/>	<input type="checkbox"/>	
12.2	Werden tägliche Betriebssicherheitsverfahren entwickelt, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren)?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Wurden Verwendungsrichtlinien für wichtige Technologien, mit denen die Mitarbeiter arbeiten (z. B. Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Notebooks, PDAs, E-Mail-Programme und Browser) entwickelt, um die korrekte Verwendung dieser Technologien für Mitarbeiter und Subunternehmer festzulegen? (b) Erfordern diese Verwendungsrichtlinien Folgendes:		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.1	Ausdrückliche Genehmigung durch das Management?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Authentifizierung zur Verwendung der Technologie?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	Liste aller solcher Geräte und Mitarbeiter mit Zugriff?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4	Etikettierung von Geräten mit Eigner, Kontaktinformationen und Zweck?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Akzeptable Verwendungen dieser Technologien?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Akzeptable Netzwerkorte für die Technologien?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.7	Liste der vom Unternehmen zugelassenen Produkte?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Aktivierung von Remotezugriffstechnologien für Anbieter nur im Bedarfsfall und mit sofortiger Deaktivierung nach der Verwendung?		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

Frage		Antwort:	Ja	Nein	Spezial*
12.3.10	Untersagt die Richtlinie bei einem Remotezugriff auf Karteninhaberdaten das Kopieren und Verschieben der Karteninhaberdaten auf lokale Festplatten und elektronische Wechselmedien sowie deren Speicherung auf diesen Medien?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Definieren die Sicherheitsrichtlinien und Verfahren klar die Informationssicherheitsverantwortung aller Mitarbeiter und Subunternehmer?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Wurden die folgenden Informationssicherheits-Managementverantwortungsbereiche einer Einzelperson oder einem Team zugewiesen?				
12.5.1	Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.2	Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das jeweilige Personal?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.4	Verwaltung von Benutzerkonten einschließlich Hinzufügen, Löschen und Ändern?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.5	Überwachung und Kontrolle des gesamten Datenzugriffs?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten zu vermitteln?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.1	Werden Mitarbeiter bei Einstellung und danach mindestens einmal im Jahr geschult?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Werden Mitarbeiter mindestens einmal pro Jahr aufgefordert, eine schriftliche Bestätigung zu geben, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens kennen?		<input type="checkbox"/>	<input type="checkbox"/>	
12.7	Werden potenzielle Mitarbeiter (siehe Definition unter Punkt 9.2) vor der Einstellung geprüft, um das Risiko interner Angriffe so gering wie möglich zu halten? <i>Für Mitarbeiter wie z. B. Kassierer und Kassiererinnen, die nur Zugriff auf jeweils eine Kartennummer gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstleistern, sofern diese ebenfalls Zugriff auf Karteninhaberdaten erhalten, umgesetzt und eingehalten und umfassen diese Richtlinien und Verfahren die folgenden Punkte?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	Führen einer Liste mit Dienstleistern		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Schriftliche Vereinbarung, die eine Bestätigung umfasst, dass die Dienstleister für die Sicherheit der Karteninhaberdaten in ihrem Besitz haften		<input type="checkbox"/>	<input type="checkbox"/>	
Frage		Antwort:	Ja	Nein	Spezial*

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

12.8.3	Festlegung eines eindeutigen Verfahrens für die Inanspruchnahme von Dienstleistern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Nutzung eines Programms zur Überwachung der Dienstleister-Konformität mit dem PCI-Datensicherheitsstandard	<input type="checkbox"/>	<input type="checkbox"/>	
12.9	Wurde ein Vorfalldaktionsplan implementiert, der eine sofortige Reaktion auf Sicherheitsverletzungen im System ermöglicht? Und umfasst dieser Plan Folgendes?			
12.9.1	(a) Wurde ein Vorfalldaktionsplan erstellt, um im Falle einer Systemsicherheitsverletzung implementiert zu werden?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Umfasst der Plan mindestens die folgenden Punkte?			
	▪ Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Konkrete Verfahren für die Reaktion auf Vorfälle	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Verfahren zur Datensicherung	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Abdeckung sämtlicher wichtigen Systemkomponenten	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.2	Wird der Plan mindestens jährlich getestet?	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.3	Steht bestimmtes Personal rund um die Uhr zur Verfügung, um auf Alarme zu reagieren?	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.4	Werden die Mitarbeiter mit Verantwortung im Bereich der Sicherheitsverletzungs-Reaktion angemessen geschult?	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.5	Werden Alarme aus Intrusionserfassungs-, -vorbeugungs- und Datei-Integritätsüberwachungssysteme eingeschlossen?	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.6	Wurde ein Prozess entwickelt und implementiert, um den Vorfalldaktionsplan je nach den gelernten Lektionen und Branchenentwicklungen zu ändern und zu aktualisieren?	<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

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

Anforderung A.1: Gemeinsam beauftragte Hosting-Anbieter müssen Karteninhaberdaten-Umgebung schützen

	Frage	Antwort:	Ja	Nein	Spezial*
A.1	<p>Werden die gehostete Umgebung und die Daten jeder Stelle (d. h. Händler, Dienstanbieter oder andere Stelle) wie in A.1.1 bis A.1.4 angegeben geschützt?</p> <p><i>Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen.</i></p> <p><i>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.</i></p>				
A.1.1	Werden an den einzelnen Stellen nur Prozesse ausgeführt, die Zugriff auf die Karteninhaberdaten-Umgebung dieser Stelle haben?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	Sind Zugriff und Rechte jeder Stelle auf die eigene Karteninhaberdaten-Umgebung beschränkt?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	Sind Protokollierungs- und Audit-Trails für die Karteninhaberdaten-Umgebung jeder Stelle aktiviert und eindeutig und entsprechen diese PCI DSS-Anforderung 10?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	Sind Prozesse implementiert, um eine rechtzeitige forensische Untersuchung zu ermöglichen, falls die Sicherheit bei einem gehosteten Händler oder Dienstanbieter verletzt wurde?		<input type="checkbox"/>	<input type="checkbox"/>	

* „Nicht zutr.“ oder „Verwendete Kompensationskontrolle“. Unternehmen, die diesen Abschnitt verwenden, müssen das Arbeitsblatt zu Kompensationskontrollen oder das Arbeitsblatt zur Nichtanwendbarkeit im Anhang ausfüllen.

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. (Die Absicht hinter den 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. 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. Beispiel: Kennwörter für den nicht über die Konsole vorgenommenen Administratorzugriff müssen 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 reduziert 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 Remotezugriff 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 Zwei-Faktoren-Authentifizierung 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) Zwei-Faktor-Authentifizierung innerhalb des internen Netzwerks.

4. 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 zu 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 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 ursprüngliche 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.	

Arbeitsblatt zu Kompensationskontrollen — Muster

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.	<i>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.</i>
2. Ziel	Definieren Sie das Ziel der ursprüngliche Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	<i>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.</i>
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	<i>Für das Zugriffskontrollsystem entsteht ein zusätzliches Risiko, da nicht gewährleistet ist, dass alle Benutzer eine eindeutige ID haben und verfolgt werden können.</i>
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	<i>Unternehmen XYZ erfordert von allen Benutzern die Anmeldung an den Servern über ihre Desktopcomputer 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.</i>
7. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	<i>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.</i>
8. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	<i>Unternehmen XYZ demonstriert 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.</i>

