



Payment Card Industry (PCI)
Datensicherheitsstandard
Selbstbeurteilungs-Fragebogen C
und Konformitätsbescheinigung

**Zahlungsanwendung mit Internet verbunden,
kein elektronischer Karteninhaberdaten-Speicher**

Version 1.2

Oktober 2008

Dokumentänderungen

Datum	Version	Beschreibung
1. Oktober 2008	1.2	Angleichen 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
Konformitätsbescheinigung, SBF C	1
Selbstbeurteilungs-Fragebogen C.....	5
Erstellung und Wartung eines sicheren Netzwerks	5
<i>Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</i>	<i>5</i>
<i>Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden</i>	<i>5</i>
Schutz von Karteninhaberdaten	6
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten.....</i>	<i>6</i>
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i>	<i>7</i>
Wartung eines Anfälligkeits-Managementprogramms.....	8
<i>Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware.....</i>	<i>8</i>
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen</i>	<i>8</i>
Implementierung starker Zugriffskontrollmaßnahmen	9
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf.....</i>	<i>9</i>
<i>Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff</i>	<i>9</i>
<i>Anforderung 9: Beschränkung des physischen Zugriff auf Karteninhaberdaten</i>	<i>9</i>
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken.....	10
<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten</i>	<i>10</i>
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse</i>	<i>10</i>
Befolgung einer Informationssicherheits-Richtlinie	11
<i>Anforderung 12: Richtlinie aufrecht erhalten, die Informationssicherheit für Mitarbeiter und Subunternehmer anspricht</i>	<i>11</i>
Anhang A: (nicht verwendet).....	12
Anhang B: Kompensationskontrollen	13
Anhang C: Arbeitsblatt zu Kompensationskontrollen.....	14
Arbeitsblatt zu Kompensationskontrollen — Muster	15
Anhang D: Erläuterung der Nichtanwendbarkeit.....	16

PCI-Datensicherheitsstandard: Damit verbundene Dokumente

Die folgenden Dokumente wurden als Hilfe für Händler und Dienstanbieter 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 Dienstanbieter
<i>PCI-DSS-Navigation: Verständnis der Intention der Anforderungen</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung</i>	Alle Händler und Dienstanbieter
<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 Dienstanbieter
<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 Dienstanbieter

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 C hat das Ziel, die Anforderungen anzusprechen, die für Händler gelten, die Karteninhaberdaten mithilfe von Zahlungsanwendungen (z. B. POS-Systemen) verarbeiten, die mit dem Internet (über Hochgeschwindigkeitsverbindung, DSL, Kabelmodem usw.) verbunden sind, aber keine Karteninhaberdaten auf einem Computersystem speichern. Diese Zahlungsanwendungen sind aus einem der folgenden Gründe mit dem Internet verbunden:

1. Die Zahlungsanwendung befindet sich auf einem mit dem Internet verbundenen PC oder
2. die Zahlungsanwendung ist mit dem Internet verbunden, um Karteninhaberdaten zu übertragen.

Diese Händler werden hier und unter *Anleitung und Richtlinien zum Selbstbeurteilungs-Fragebogen* als SBF-Validierungstyp 4 definiert. Händler des Validierungstyps 4 verarbeiten Karteninhaberdaten über POS-Systeme, die mit dem Internet verbunden sind, und speichern Karteninhaberdaten nicht auf einem Computersystem. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder E-Commerce- bzw. Post-/Telefonbestellungshändler (Karte liegt nicht vor) handeln. Diese Händler müssen die Konformität durch Ausfüllen von SBF C und der damit verbundenen Konformitätsbescheinigung validieren, wodurch sie Folgendes bestätigen:

- Ihr Unternehmen hat auf dem gleichen Gerät ein Zahlungssystem und eine Internetverbindung.
- Das Gerät mit Zahlungsanwendung/Internetverbindung ist nicht mit anderen Systemen in Ihrer Umgebung verbunden.
- Ihr Unternehmen bewahrt nur Berichte oder Kopien der Quittungen auf Papier auf.
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format und
- der Anbieter der Zahlungsanwendung Ihres Unternehmens verwendet sichere Techniken zur Bereitstellung von Remote-Unterstützung für Ihr Zahlungssystem.

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 C) 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 Konformitätsbescheinigung komplett aus.
4. Reichen Sie den SBF, den Nachweis eines bestandenen Scans und die Konformitätsbescheinigung zusammen mit allen anderen erforderlichen Dokumenten bei Ihrem Acquirer ein.

Anweisungen zur Nichtanwendbarkeit und zum bestimmter Anforderungen

Ausschluss: Wenn Sie SBF C ausfüllen müssen, um Ihre PCI-DSS-Konformität zu bestätigen, kann folgende Ausnahme berücksichtigt werden: Siehe „Nichtanwendbarkeit“ für die entsprechende SFB-Antwort.

- Die für drahtlose Technologie spezifischen Fragen müssen nur beantwortet werden, wenn drahtlose Technologie in Ihrem Netzwerk verwendet wird (z. B. Anforderung 2.1.1). 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.

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.

Konformitätsbescheinigung, SBF C

Anleitung zum Einreichen

Der Händler muss diese Konformitätsbescheinigung einreichen, um zu bestätigen, dass er den Konformitätsstatus mit den *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 des qualifizierten Sicherheitsprüfers (falls vorhanden)

Name des Unternehmens:			
QSA-Leiter:		Titel:	
Telefonnr.:		E-Mail:	
Geschäftsadresse:		Ort:	
Bundesstaat/Provinz:		Land:	PLZ: <input type="text"/>
URL:			

Teil 2. Informationen zum Händlerunternehmen

Name des Unternehmens:		DBA(S):	
Name des Ansprechpartners:		Titel:	
Telefonnr.:		E-Mail:	
Geschäftsadresse:		Ort:	
Bundesstaat/Provinz:		Land:	PLZ: <input type="text"/>
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 2d. Qualifikation zum Ausfüllen von SBF C

Der Händler bestätigt die Qualifikation zum Ausfüllen dieser abgekürzten Version des Selbstbeurteilungs-Fragebogens aus folgenden Gründen:

<input type="checkbox"/>	Der Händler hat auf dem gleichen Gerät ein Zahlungsanwendungssystem und eine Verbindung mit dem Internet oder einem öffentlichen Netz.
<input type="checkbox"/>	Das Gerät mit Zahlungsanwendungssystem/Internetverbindung ist nicht mit anderen Systemen in der Händlerumgebung verbunden.
<input type="checkbox"/>	Der Händler speichert keine Karteninhaberdaten in elektronischem Format.
<input type="checkbox"/>	Wenn der Händler Karteninhaberdaten speichert, befinden sich diese nur in Berichten oder Kopien von Quittungen auf Papier und werden nicht elektronisch entgegen genommen.
<input type="checkbox"/>	Der Anbieter der Zahlungsanwendungssoftware des Händlers verwendet sichere Techniken zur Bereitstellung von Remote-Unterstützung für das Zahlungsanwendungssystem des Händlers.

Teil 3. PCI-DSS-Validierung

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

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

<input type="checkbox"/>	PCI-DSS Selbstbeurteilungs-Fragebogen C, Version (<i>version of SAQ</i>), wurde den enthaltenen Anleitungen gemäß ausgefüllt.
<input type="checkbox"/>	Alle Informationen im oben genannten SBF und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung in allen materiellen Aspekten korrekt dar.
<input type="checkbox"/>	Mein Zahlungsanwendungsanbieter hat mir bestätigt, dass in meinem Zahlungssystem nach der Autorisierung keine empfindlichen Authentifizierungsdaten gespeichert werden.
<input type="checkbox"/>	Ich habe den PCI-DSS gelesen und bestätige, dass ich jederzeit meine volle PCI-DSS-Konformität haben muss.
<input type="checkbox"/>	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifen­daten (aus einer Spur) ² , CAV2-, CVC2-, CID-, CVV2-Daten ³ oder PIN-Daten ⁴ gespeichert wurden.

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 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 ↑

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 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	Konformitätsstatus (eine Option auswählen)		Abhilfedatum und Aktionen (bei Konformitätsstatus „Keine Konformität“)
		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"/>	
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 C

Ausfülldatum:

Erstellung und Wartung eines sicheren Netzwerks

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

Frage	Antwort:	Ja	Nein	Spezial*
1.2 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>		<input type="checkbox"/>	<input type="checkbox"/>	
1.3 Verbietet die Firewall-Konfiguration den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung?		<input type="checkbox"/>	<input type="checkbox"/>	

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 Standardseinstellungen 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"/>	
2.3 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.

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
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 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. <i>Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:</i> <ul style="list-style-type: none"> ▪ Name des Karteninhabers ▪ Primary Account Number (PAN), ▪ Ablaufdatum und ▪ Servicecode <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> <i>Hinweis: Weitere Informationen finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2 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. <i>Hinweis: Weitere Informationen finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3 Keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blocks speichern.		<input type="checkbox"/>	<input type="checkbox"/>	
3.3 Ist die PAN bei der Anzeige maskiert (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden)? <i>Hinweise:</i> <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"/>	

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

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

	Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
4.1	<p>Werden eine starke Kryptographie sowie Sicherheitsprotokolle wie SSL/TLS oder IPSEC verwendet, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen?</p> <p><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></p> <p><i>Hinweis: Bitte beachten Sie Folgendes, wenn Sie in Ihrer Umgebung eine Wireless-Technologie implementiert haben:</i></p> <ul style="list-style-type: none"> ▪ <i>Für neue drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 31. März 2009 zu implementieren.</i> ▪ <i>Für bestehende drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 30. Juni 2010 zu implementieren.</i> 	<input type="checkbox"/>	<input type="checkbox"/>		
4.2	<p>Existieren Richtlinien, Verfahren und Praktiken, um das Senden unverschlüsselter PANs mittels Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat) auszuschließen?</p>	<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.

Wartung eines Anfälligkeits-Managementprogramms

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware

Frage		Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
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:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
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"/>	

* „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"/>	

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

Frage	Antwort:	Ja	Nein	Spezial*
8.5.6 Sind von Lieferanten für die Remote-Pflege verwendete Accounts nur während der erforderlichen Zeit aktiviert?		<input type="checkbox"/>	<input type="checkbox"/>	

Anforderung 9: Beschränkung des physischen Zugriff auf Karteninhaberdaten

Frage	Antwort:	Ja	Nein	Spezial*
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"/>	
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"/>	
9.10 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"/>	

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

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

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

Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
Keine Fragen für SBF C zutreffend.				

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

Frage	Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
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"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Befolgung einer Informationssicherheits-Richtlinie

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

Frage		Antwort:	<u>Ja</u>	<u>Nein</u>	<u>Spezial*</u>
12.1	Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und verbreitet und hat sie Folgendes erreicht:		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Umfasst eine Überprüfung mindestens einmal im Jahr und Aktualisierungen bei Umgebungsänderungen?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Wurden Verwendungsrichtlinien für wichtige Technologien, mit denen die Mitarbeiter arbeiten (z. B. Remote-Zugriffs- und Wireless-Technologien, elektronische Wechselmedien, Notebooks, PDAs, E-Mail-Programme und Browser) entwickelt, um die korrekte Verwendung dieser Technologien für Mitarbeiter und Subunternehmer festzulegen?		<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?				
12.5.3	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"/>	
12.6	Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten zu vermitteln?		<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"/>	
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"/>	

* „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: (nicht verwendet)

Die restliche Seite wurde absichtlich frei gelassen.

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, das 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 Zwei-Faktoren-Authentifizierung ist eine akzeptable Kompensationkontrolle, 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>

