



Payment Card Industry (PCI)
Datensicherheitsstandard
**Selbstbeurteilungsfragebogen B
und Konformitätsbescheinigung**

**Nur Abdruckgeräte oder eigenständige
Terminals mit Dial-Out-Funktion, kein
elektronischer Karteninhaberdaten-Speicher**

Version 2.0

Oktober 2010

Dokumentänderungen

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

Inhalt

Dokumentänderungen	i
PCI-Datensicherheitsstandard: Zugehörige Dokumente	iii
Vorbereitung.....	iv
Ausfüllen des Selbstbeurteilungsfragebogens	iv
PCI-DSS-Konformität – Schritte zum Ausfüllen.....	iv
Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen	iv
Konformitätsbescheinigung, SBF B	1
Selbstbeurteilungsfragebogen B	5
Schutz von Karteninhaberdaten.....	5
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i>	<i>5</i>
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i>	<i>6</i>
Implementierung starker Zugriffskontrollmaßnahmen	7
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf.....</i>	<i>7</i>
<i>Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken.....</i>	<i>7</i>
Befolgung einer Informationssicherheitsrichtlinie.....	9
<i>Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.....</i>	<i>9</i>
Anhang A: (findet keine Anwendung)	11
Anhang B: Kompensationskontrollen	12
Anhang C: Kompensationskontrollen – Arbeitsblatt	14
Arbeitsblatt – Kompensationskontrollen – Beispiel.....	15
Anhang D: Erläuterung der Nichtanwendbarkeit	17

PCI-Datensicherheitsstandard: Zugehörige Dokumente

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

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

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

Vorbereitung

Ausfüllen des Selbstbeurteilungsfragebogens

SBF B wurde entwickelt, um die Anforderungen an Händler anzusprechen, die Karteninhaberdaten nur mithilfe von Abdruckgeräten oder eigenständigen Terminals mit Dial-Out-Funktion verarbeiten.

SBF B-Händler werden hier und in der *Anleitung und den Richtlinien zum PCI-DSS-Selbstbeurteilungsfragebogen* definiert. SBF B-Händler verarbeiten Karteninhaberdaten nur über eigenständige Abdruckmaschinen oder Terminals mit Dial-Out-Funktion. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder E-Commerce- bzw. Versandhändler (Karte liegt nicht vor) handeln. Diese Händler bestätigen die Einhaltung der Anforderungen, indem sie den SBF B und die damit verbundenen Konformitätsbescheinigung ausfüllen und darin Folgendes bestätigen:

- Ihr Unternehmen verwendet ausschließlich Abdruckgeräte und/oder eigenständige Terminals mit Dial-Out-Funktion (über eine Telefonleitung mit Ihrem Prozessor verbunden), um die Zahlungskarteninformationen Ihrer Kunden zu erfassen;
- Die eigenständigen Terminals mit Dial-Out-Funktion sind nicht mit anderen Systemen in Ihrer Umgebung verbunden.
- Die eigenständigen Terminals mit Dial-Out-Funktion sind nicht mit dem Internet verbunden.
- Ihr Unternehmen überträgt keine Karteninhaberdaten über Netzwerke (weder interne Netzwerke noch über das Internet);
- Ihr Unternehmen bewahrt ausschließlich Papierdokumente oder Kopien von Quittungen mit Karteninhaberdaten auf und diese Dokumente werden nicht elektronisch entgegengenommen;
und
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Alle Abschnitte des Fragebogens konzentrieren sich auf einen bestimmten Sicherheitsbereich und basieren auf den *PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren*. Diese verkürzte Version des SBF beinhaltet Fragen, die für eine bestimmte Art von Umgebungen kleiner Handelsunternehmen, so wie in den Qualifikationskriterien oben definiert, gelten. Sollten für Ihre Umgebung PCI-DSS-Anforderungen gelten, die nicht in diesem SBF behandelt werden, kann dies ein Hinweis darauf sein, dass dieser SBF nicht für Ihr Unternehmen geeignet ist. Zusätzlich müssen Sie auch weiterhin alle geltenden PCI-DSS-Anforderungen erfüllen, um als PCI-DSS-konform angesehen zu werden.

PCI-DSS-Konformität – Schritte zum Ausfüllen

1. Bewerten Sie Ihre Umgebung auf die Einhaltung des PCI-DSS.
2. Füllen Sie den Selbstbeurteilungsfragebogen (SBF B) gemäß den Anweisungen in der *Anleitung und den Richtlinien zum Selbstbeurteilungsfragebogen* aus.
3. Füllen Sie die Konformitätsbescheinigung vollständig aus.
4. Reichen Sie den SBF und die Konformitätsbescheinigung zusammen mit allen anderen erforderlichen Dokumenten bei Ihrem Acquirer ein.

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

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

Konformitätsbescheinigung, SBF B

Anleitung zum Einreichen

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

Teil 1. Informationen zum qualifizierten Sicherheitsprüfer

Teil 1a. Informationen zum Händlerunternehmen

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

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

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

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

- Einzelhändler
 Telekommunikation
 Lebensmittel und Supermärkte
 Erdöl/Erdgas
 E-Commerce
 Versandhandel
 Sonstige Unternehmen (bitte angeben):

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

Teil 2a. Beziehungen

Steht Ihr Unternehmen in Beziehung zu einem oder mehreren Drittdienstleistern (z. B. Gateways, Webhosting-Unternehmen, Buchungspersonal von Fluggesellschaften, Vertreter von Kundentreueprogrammen usw.)? Ja Nein

Steht Ihr Unternehmen mit mehr als einem Acquirer in Kontakt? Ja Nein

Teil 2b. Transaktionsverarbeitung

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

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

<u>Verwendete Zahlungsanwendung</u>	<u>Versionsnummer</u>	<u>Letzte Validierung gemäß PABP/PA-DSS</u>

Teil 2c. Qualifikation zum Ausfüllen des SBF B

Der Händler bestätigt die Qualifikation zum Ausfüllen dieser abgekürzten Version des Selbstbeurteilungsfragebogens aus folgenden Gründen:

- Der Händler verwendet ausschließlich eine Abdruckmaschine, um einen Abdruck der Zahlungskarteninformationen des Kunden zu erhalten, und überträgt Karteninhaberdaten weder über eine Telefonleitung noch über das Internet; oder
Der Händler verwendet ausschließlich eigenständige Dial-Out-Terminals, welche nicht mit dem Internet oder anderen Systemen in der Händlerumgebung verbunden sind;
- Der Händler speichert keine Karteninhaberdaten in elektronischem Format; **und**
- Wenn der Händler Karteninhaberdaten speichert, befinden sich diese nur in Berichten oder Kopien von Quittungen auf Papier und werden nicht elektronisch entgegengenommen.

Teil 3. PCI-DSS-Validierung

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

- Konform:** Alle Abschnitte des PCI SBF sind komplett und alle Fragen wurden mit „Ja“ beantwortet, woraus sich die Gesamtbewertung **KONFORM** ergeben und (*Name des Händlerunternehmens*) volle Konformität mit dem PCI-DSS gezeigt hat.
- Nicht konform:** Nicht alle Abschnitte des PCI SBF sind komplett und einige Fragen wurden mit „Nein“ beantwortet, woraus sich die Gesamtbewertung **NICHT KONFORM** ergeben und (*Name des Händlerunternehmens*) nicht die volle Konformität mit dem PCI-DSS gezeigt hat.
Zieldatum für Konformität:
Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

Teil 3a. Bestätigung des Status „Konform“

Händler bestätigt:

<input type="checkbox"/>	PCI-DSS Selbstbeurteilungsfragebogen B, Version (<i>Version des SBF</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 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 erkenne an, dass ich jederzeit die vollständige PCI-DSS-Konformität aufrechterhalten 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- oder CVV2-Daten ³ oder PIN-Daten ⁴ gespeichert wurden.

Teil 3b. Bestätigung durch den 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 oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Spurdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

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

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

PCI-DSS-Anforderung	Anforderungsbeschreibung	Konformitätsstatus (eine Option auswählen)		Abhilfedatum und Aktionen (bei Konformitätsstatus „NEIN“)
		JA	NEIN	
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"/>	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	<input type="checkbox"/>	<input type="checkbox"/>	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	<input type="checkbox"/>	<input type="checkbox"/>	
12	Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.	<input type="checkbox"/>	<input type="checkbox"/>	

Selbstbeurteilungsfragebogen B

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

Ausfülldatum:

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

PCI-DSS Frage	Antwort:	Ja	Nei n	Spezial*
3.2 (b) Falls vertrauliche Authentifizierungsdaten empfangen und gelöscht werden, sind Prozesse zum Löschen der Daten vorhanden, um sicherzustellen, dass die Daten nicht wiederhergestellt werden können?		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Halten alle Systeme die folgenden Anforderungen hinsichtlich des Verbots, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern, ein (auch wenn diese verschlüsselt sind)?				
3.2.1 Wird der gesamte Inhalt einer Spur auf dem Magnetstreifen (auf der Rückseite einer Karte, gleichwertige Daten auf einem Chip oder an einer anderen Stelle) tatsächlich nicht gespeichert? Diese Daten werden auch als Full Track, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet. <i>Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente des Magnetstreifens gespeichert werden:</i> <ul style="list-style-type: none"> ▪ Der Name des Karteninhabers, ▪ Primäre Kontonummer (PAN), ▪ Ablaufdatum und ▪ Servicecode <i>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2 Wird der Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte) tatsächlich nicht gespeichert?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3 Werden persönliche Identifizierungsnummern (PIN) oder verschlüsselte PIN-Blocks tatsächlich nicht gespeichert?		<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 die vollständige PAN aus betrieblichen Gründen einsehen müssen. ▪ Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. für POS-Belege. 		<input type="checkbox"/>	<input type="checkbox"/>	

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

PCI-DSS Frage		Antwort:	<u>Ja</u>	<u>Nei</u> <u>n</u>	<u>Spezial</u> *
4.2	(b) Sind Richtlinien vorhanden, die festlegen, dass ungeschützte PANs nicht über Messaging-Technologien für Endanwender gesendet werden dürfen?		<input type="checkbox"/>	<input type="checkbox"/>	

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

PCI-DSS Frage	Antwort:	Ja	Nei n	Spezial*
7.1 Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten wie folgt ausschließlich auf jene Personen beschränkt, deren Tätigkeit diesen Zugriff erfordert?				
7.1.1 Sind die Zugriffsrechte für Benutzernamen auf Mindestberechtigungen beschränkt, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2 Werden Berechtigungen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen (auch als „rollenbasierte Zugriffssteuerung“ oder RBAC bezeichnet)?		<input type="checkbox"/>	<input type="checkbox"/>	

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

PCI-DSS Frage	Antwort:	Ja	Nei n	Spezial*
9.6 Wird die physische Sicherheit aller Medien gewährleistet (einschließlich, aber nicht beschränkt auf Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)? <i>Zum Zwecke der Anforderung 9, bezieht sich der Begriff „Medien“ auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
9.7 (a) Wird die interne oder externe Verteilung jeglicher Art von Medien stets strikt kontrolliert?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Umfassen die Kontrollen folgende Punkte?				
9.7.1 Werden Medien klassifiziert, sodass die Sensibilität der Daten bestimmt werden kann?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2 Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8 Werden Protokolle geführt, um Medien zurückverfolgen zu können, die aus einem gesicherten Bereich heraus verlagert wurden, und muss für eine solche Verlagerung zunächst die Genehmigung des Managements eingeholt werden (insbesondere wenn Medien an Einzelpersonen verteilt werden)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9 Werden strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durchgeführt?		<input type="checkbox"/>	<input type="checkbox"/>	

PCI-DSS Frage		Antwort:	<u>Ja</u>	<u>Nei</u> <u>n</u>	<u>Spezial</u> *
9.10	Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?		<input type="checkbox"/>	<input type="checkbox"/>	
	Erfolgt die Vernichtung von Daten wie nachstehend beschrieben?				
9.10.1	(a) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Werden Container, die Daten beinhalten, welche gelöscht werden sollen, entsprechend geschützt, um Zugriffe auf diese Inhalte zu vermeiden? (Wird ein Container mit zu vernichtenden Akten beispielsweise durch ein Schloss geschützt, um Zugriffe auf den Inhalt zu vermeiden?)		<input type="checkbox"/>	<input type="checkbox"/>	

Befolgung einer Informationssicherheitsrichtlinie

Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal

PCI-DSS Frage		Antwort:	Ja	Nei n	Spezial*
12.1	<p>Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und an das betroffene Personal weitergeleitet?</p> <p><i>Zum Zwecke der Anforderung 12 bezieht sich der Begriff „Mitarbeiter“ hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Stelle „ansässig“ sind oder anderweitig Zugriff auf die Karteninhaberdaten-Umgebung haben.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Wird die Richtlinie zur Informationssicherheit mindestens einmal im Jahr überarbeitet und an die geänderten Geschäftsziele bzw. Risiken angepasst?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	Wurden Verwendungsrichtlinien für wichtige Technologien (z. B. Remote-Zugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, PDAs, E-Mail-Programme und Internet) entwickelt, welche allen Mitarbeitern die korrekte Verwendung dieser Technologien erläutern und folgende Punkte voraussetzen?				
12.3.1	Ausdrückliche Genehmigung durch autorisierte Parteien, diese Technologien zu benutzen;		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	Eine Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriffsrechten;		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Akzeptable Verwendungen dieser Technologien.		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?				
12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten zu vermitteln?		<input type="checkbox"/>	<input type="checkbox"/>	

PCI-DSS Frage		Antwort:		
		<u>Ja</u>	<u>Nei n</u>	<u>Spezial*</u>
12.8	Falls Dienstleister Zugriff auf Karteninhaberdaten haben, werden wie folgt Richtlinien zur Verwaltung von Dienstleistern umgesetzt und eingehalten?			
12.8.1	Wird eine Liste der Dienstleister geführt?	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Existiert eine schriftliche Vereinbarung mit einer Bestätigung, dass der Dienstleister für die Sicherheit der Karteninhaberdaten in seinem Besitz haftet?	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Gibt es ein eindeutiges Verfahren 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	Wird ein Programm zur Überwachung der Dienstleister-Konformität mit dem PCI-Datensicherheitsstandard eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	

Anhang A: (findet keine Anwendung)

Diese 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. (Der Zweck der einzelnen PCI-DSS-Anforderungen ist unter *PCI-DSS-Navigation* erläutert.)
3. Sie müssen mindestens so weitreichend wie andere PCI-DSS-Anforderungen sein. (Die reine Konformität mit anderen PCI-DSS-Anforderungen reicht als Kompensation nicht aus.)

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

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

- a) Vorhandene PCI-DSS-Anforderungen können NICHT als Kompensationskontrollen betrachtet werden, wenn sie für das in Frage kommende Element ohnehin erforderlich sind. Zum Beispiel müssen Kennwörter für den nicht über die Konsole vorgenommenen Administratorzugriff verschlüsselt versendet werden, damit Administratorkennwörter nicht von Unbefugten abgefangen werden können. Als Kompensation für eine fehlende Kennwortverschlüsselung können nicht andere PCI-DSS-Kennwortanforderungen wie das Aussperren von Eindringlingen, die Einrichtung komplexer Kennwörter usw. ins Feld geführt werden, da sich mit diesen Anforderungen das Risiko eines Abfangens unverschlüsselter Kennwörter nicht reduzieren lässt. Außerdem sind die anderen Kennwortkontrollen bereits Bestandteil der PCI-DSS-Anforderungen für das betreffende Element (Kennwort).
- b) Vorhandene PCI-DSS-Anforderungen können EVENTUELL als Kompensationskontrollen betrachtet werden, wenn sie zwar für einen anderen Bereich, nicht aber für das in Frage kommende Element erforderlich sind. Beispiel: Beim Remote-Zugriff ist nach PCI-DSS eine Authentifizierung anhand zweier Faktoren erforderlich. Die Authentifizierung anhand zweier Faktoren *innerhalb des internen Netzwerks* kann für den nicht über die Konsole stattfindenden Administratorzugriff als Kompensationskontrolle betrachtet werden, wenn eine Übertragung verschlüsselter Kennwörter nicht möglich ist. Die Authentifizierung anhand zweier Faktoren ist eine akzeptable Kompensationskontrolle, wenn (1) die Absicht der ursprünglichen Anforderung erfüllt wird (das Risiko des Abfangens unverschlüsselter Kennwörter wird verhindert) und (2) die Authentifizierung in einer sicheren Umgebung ordnungsgemäß konfiguriert wurde.
- c) Die vorhandenen PCI-DSS-Anforderungen können mit neuen Kontrollen zusammen als Kompensationskontrolle fungieren. Beispiel: Ein Unternehmen kann Karteninhaberdaten nicht nach Anforderung 3.4 unlesbar machen (z. B. durch Verschlüsselung). In diesem Fall könnte eine Kompensation darin bestehen, dass mit einem Gerät bzw. einer Kombination aus Geräten, Anwendungen und Kontrollen folgende Punkte sichergestellt sind: (1) Interne Netzwerksegmentierung; (2) Filtern von IP- oder MAC-Adressen und (3) Authentifizierung anhand zweier Faktoren innerhalb des internen Netzwerks.

4. Anpassung an das zusätzliche Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht.

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 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: Kompensationskontrollen – Arbeitsblatt

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

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

Anforderungsnummer und -definition:

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

Arbeitsblatt – Kompensationskontrollen – Beispiel

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

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

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	<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 ursprünglichen 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 Desktop-Computer unter Verwendung des Befehls SU. SU ermöglicht einem Benutzer den Zugriff auf das Konto „root“ und die Durchführung von Aktionen unter dem Konto „root“, wobei der Vorgang im Verzeichnis „SU-log“ protokolliert werden kann. Auf diese Weise können die Aktionen der einzelnen Benutzer über das SU-Konto verfolgt werden.</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	<i>Unternehmen XYZ demonstriert Prozesse und Verfahren, mit denen sichergestellt wird, dass SU-Konfigurationen nicht durch</i>

	Kompensationskontrollen fest.	<i>Änderung, Bearbeitung oder Löschen so bearbeitet werden können, dass eine Ausführung von „root“-Befehlen ohne individuelle Benutzerverfolgung bzw. Protokollierung möglich würde.</i>
--	-------------------------------	--

