

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

---

**Alle Karteninhaberdaten-Funktionen wurden  
ausgegliedert. Keine elektronische Speicherung,  
Verarbeitung oder Übertragung von  
Karteninhaberdaten**

**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 nach der Ursprungsversion v1.1.
28. Oktober 2010	2.0	Anpassung der Inhalte an die neuen PCI-DSS v2.0 Anforderungen und Prüfverfahren.

## Inhalt

---

<b>Dokumentänderungen .....</b>	<b>i</b>
<b>PCI-Datensicherheitsstandard: Zugehörige Dokumente .....</b>	<b>ii</b>
<b>Vorbereitung .....</b>	<b>iii</b>
<b>Ausfüllen des Selbstbeurteilungsfragebogens .....</b>	<b>iii</b>
<b>PCI-DSS-Konformität – Schritte zum Ausfüllen.....</b>	<b>iii</b>
<b>Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen .....</b>	<b>iii</b>
<b>Konformitätsbescheinigung, SBF A .....</b>	<b>1</b>
<b>Selbstbeurteilungsfragebogen A .....</b>	<b>4</b>
<b>Implementierung starker Zugriffskontrollmaßnahmen .....</b>	<b>4</b>
<i>Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken.....</i>	<i>4</i>
<b>Befolgung einer Informationssicherheitsrichtlinie.....</b>	<b>5</b>
<i>Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal .....</i>	<i>5</i>
<b>Anhang A: (findet keine Anwendung) .....</b>	<b>6</b>
<b>Anhang B: Kompensationskontrollen .....</b>	<b>7</b>
<b>Anhang C: Kompensationskontrollen – Arbeitsblatt .....</b>	<b>9</b>
<b>Kompensationskontrollen – Arbeitsblatt – Beispiel.....</b>	<b>10</b>
<b>Anhang D: Erläuterung der Nichtanwendbarkeit .....</b>	<b>12</b>

## PCI-Datensicherheitsstandard: Zugehörige Dokumente

Die folgenden Dokumente wurden als Unterstützung für Händler und Dienstanbieter entwickelt, um sie 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 des 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 <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen B und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen C-VT und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen C und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen D und Bescheinigung</i>	Qualifizierte Händler und Dienstanbieter <sup>1</sup>
<i>PCI-Datensicherheitsstandard und Datensicherheitsstandard für Zahlungsanwendungen: Glossar für Begriffe, Abkürzungen und Akronyme</i>	Alle Händler und Dienstanbieter

<sup>1</sup> 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 A wurde entwickelt, um die Anforderungen an Händler anzusprechen, die nur Papierdokumente oder -quittungen mit Karteninhaberdaten aufbewahren, keine Karteninhaberdaten in elektronischer Form speichern und vor Ort oder auf ihren Systemen keine Karteninhaberdaten verarbeiten oder übertragen.

SBF A-Händler, die hier und unter der *Anleitung und den Richtlinien zum PCI-DSS-Selbstbeurteilungsfragebogen* definiert werden, speichern keine Karteninhaberdaten in elektronischem Format und verarbeiten oder übertragen weder vor Ort noch auf ihren Systemen Karteninhaberdaten. Diese Händler müssen die Einhaltung der Anforderungen bestätigen, indem sie den SBF A und die zugehörige Konformitätsbescheinigung ausfüllen und darin Folgendes bestätigen:

- Ihr Unternehmen führt nur Transaktionen durch, bei denen die Karte nicht physisch vorliegt (E-Commerce oder Versandhandel).
- Ihr Unternehmen speichert, verarbeitet oder überträgt keine Karteninhaberdaten, weder vor Ort noch auf Ihren Systemen, sondern verlässt sich voll und ganz auf einen oder mehrere Drittdienstleister, der/die diese Funktionen übernimmt/übernehmen;
- Ihr Unternehmen hat bestätigt, dass die Handhabung, Speicherung, Verarbeitung bzw. Übertragung der Karteninhaberdaten durch das oder die Drittunternehmen den PCI-DSS erfüllen.
- Ihr Unternehmen bewahrt ausschließlich Papierdokumente oder -quittungen mit Karteninhaberdaten auf und diese Dokumente werden nicht elektronisch entgegengenommen;  
**und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

**Diese Option gilt nicht für Händler in einer physischen POS-Umgebung (persönlicher Publikumsverkehr).**

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 A) gemäß 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 A

## 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  
  Lebensmitteleinzelhandel und Supermärkte  
 Erdöl/Erdgas  
  E-Commerce  
  Versandhandel  
  Sonstiges (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. Qualifikation zum Ausfüllen des SBF A

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

<input type="checkbox"/>	Der Händler speichert, verarbeitet oder überträgt keine Karteninhaberdaten, weder vor Ort noch auf seinen Systemen, sondern verlässt sich voll und ganz auf einen oder mehrere Drittdienstleister, der/die diese Funktionen übernimmt/übernehmen;
<input type="checkbox"/>	Es wurde bestätigt, dass die Handhabung, Speicherung, Verarbeitung bzw. Übertragung der Karteninhaberdaten durch den Drittdienstleister den PCI-DSS erfüllen.
<input type="checkbox"/>	Der Händler speichert keine Karteninhaberdaten in elektronischem Format; <b>und</b>
<input type="checkbox"/>	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 A mit Datum vom (*Ausfülldatum*) notiert wurden, bestätigt (*Name des Händlerunternehmens*) folgenden Konformitätsstatus (eine Option auswählen):

<input type="checkbox"/>	<b>Konform:</b> Alle Abschnitte des PCI SBF sind vollständig und alle Fragen wurden mit „Ja“ beantwortet, woraus sich die Gesamtbewertung <b>KONFORM</b> ergeben und ( <i>Name des Händlerunternehmens</i> ) volle Konformität mit dem PCI-DSS gezeigt hat.
<input type="checkbox"/>	<b>Nicht konform:</b> Nicht alle Abschnitte des PCI SBF sind vollständig und einige Fragen wurden mit „Nein“ beantwortet, woraus sich die Gesamtbewertung <b>NICHT KONFORM</b> ergeben und ( <i>Name des Händlerunternehmens</i> ) nicht die volle Konformität mit dem PCI-DSS gezeigt hat. <ul style="list-style-type: none"> <li>▪ <b>Zieldatum</b> für Konformität:</li> <li>▪ Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. <i>Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.</i></li> </ul>

### Teil 3a. Bestätigung des Status „Konform“

Der Händler bestätigt:

<input type="checkbox"/>	Der PCI-DSS Selbstbeurteilungsfragebogen A, Version ( <i>SBF Versionsnr.</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"/>	Ich habe den PCI-DSS gelesen und erkenne an, dass ich jederzeit die vollständige PCI-DSS-Konformität aufrechterhalten muss.

### Teil 3b. Bestätigung durch den Händler

Unterschrift des Beauftragten des Händlers ↑	Datum ↑

Name des Beauftragten des Händlers ↑

Titel ↑

Vertretenes Händlerunternehmen ↑

#### Teil 4. Aktionsplan für Status „Nicht konform“

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

PCI-DSS-Anforderung	Anforderungsbeschreibung	Konformitätsstatus (eine Option auswählen)		Abhilfedatum und Aktionen (bei Konformitätsstatus „NEIN“)
		JA	NEIN	
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 A

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

Ausfülldatum:

### Implementierung starker Zugriffskontrollmaßnahmen

#### 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"/>	
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:		Spezial*
		Ja	Nei n	
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 aufwiegt. (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 gemäß 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. <b>Einschränkungen</b>	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	
2. <b>Ziel</b>	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
3. <b>Ermitteltes Risiko</b>	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
4. <b>Definition der Kompensationskontrollen</b>	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. <b>Validierung der Kompensationskontrollen</b>	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. <b>Verwaltung</b>	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

## Kompensationskontrollen – Arbeitsblatt – Beispiel

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

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

	Erforderliche Informationen	Erklärung
<b>1. Einschränkungen</b>	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>
<b>2. Ziel</b>	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>
<b>3. Ermitteltes Risiko</b>	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>
<b>4. Definition der Kompensationskontrollen</b>	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>
<b>5. Validierung der Kompensationskontrollen</b>	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>
<b>6. Verwaltung</b>	Legen Sie Prozesse und Kontrollen zur Verwaltung der	<i>Unternehmen XYZ dokumentiert 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>
--	-------------------------------	--

