



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

**Keine elektronische Speicherung, Verarbeitung
oder Übertragung von Karteninhaberdaten**

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	ii
Vorbereitung.....	iii
Ausfüllen des Selbstbeurteilungs-Fragebogens	iii
PCI-DSS-Konformität – Schritte zum Ausfüllen.....	iii
Anweisungen zur Nichtanwendbarkeit bestimmter Anforderungen	iii
Konformitätsbescheinigung, SBF A.....	1
Selbstbeurteilungs-Fragebogen A.....	4
Implementierung starker Zugriffskontrollmaßnahmen	4
<i>Anforderung 9: Beschränkung des physischen Zugriff auf Karteninhaberdaten.....</i>	<i>4</i>
Befolgung einer Informationssicherheits-Richtlinie	5
<i>Anforderung 12: Richtlinie aufrecht erhalten, die Informationssicherheit für Mitarbeiter und Subunternehmer anspricht</i>	<i>5</i>
Anhang A: (nicht verwendet)	6
Anhang B: Kompensationskontrollen.....	7
Anhang C: Arbeitsblatt zu Kompensationskontrollen.....	9
Arbeitsblatt zu Kompensationskontrollen – Beispiel.....	10
Anhang D: Erläuterung der Nichtanwendbarkeit	11

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 DSS 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 A wurde entwickelt, um die Anforderungen an Händler anzusprechen, die nur Papierdokumente oder -quittungen mit Karteninhaberdaten führen, Karteninhaberdaten nicht in elektronischem Format speichern und vor Ort keine Karteninhaberdaten verarbeiten oder übertragen.

Diese Händler, die hier und unter Anleitung und Richtlinien zum PCI-DSS-Selbstbeurteilungs-Fragebogen als SBF-Validierungstyp 1 definiert werden, speichern keine Karteninhaberdaten in elektronischem Format und verarbeiten oder übertragen vor Ort keine Karteninhaberdaten. Diese Händler müssen die Konformität durch Ausfüllen von SBF A und der damit verbundenen Konformitätsbescheinigung validieren, wodurch sie Folgendes bestätigen:

- Ihr Unternehmen führt nur Transaktionen durch, bei denen die Karte nicht physisch vorliegt (E-Commerce oder Bestellungen per Post/Telefon).
- Ihr Unternehmen speichert, verarbeitet oder überträgt keine Karteninhaberdaten vor Ort, sondern verlässt sich ganz auf einen oder mehrere Drittdienstanbieter, der/die diese Funktionen übernimmt/übernehmen.
- Ihr Unternehmen hat bestätigt, dass die Handhabung, Speicherung, Verarbeitung bzw. Übertragung der Karteninhaberdaten durch den Drittdienstanbieter den PCI-DSS erfüllt.
- Ihr Unternehmen bewahrt nur Papierdokumente oder -quittungen mit Karteninhaberdaten auf, und diese Dokumente werden nicht elektronisch empfangen **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Diese Option würde nie für Händler in einer physischen POS-Umgebung (persönlicher Publikumsverkehr) gelten.

PCI-DSS-Konformität – Schritte zum Ausfüllen

1. Füllen Sie den Selbstbeurteilungs-Fragebogen (SBF A) gemäß den Anweisungen unter *Anleitung und Richtlinien zum Selbstbeurteilungs-Fragebogen* aus.
2. Füllen Sie die Konformitätsbescheinigung komplett aus.
3. Reichen Sie den SBF und die Konformitätsbescheinigung zusammen mit allen anderen erforderlichen Dokumenten bei Ihrem Acquirer ein.

Anweisungen zur Nichtanwendbarkeit bestimmter Anforderungen

Nichtanwendbarkeit: 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 A

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:	
URL:					

Teil 2. Informationen zum Händlerunternehmen

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

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

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

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

Teil 2b. Beziehungen

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

Ja Nein

Hat Ihr Unternehmen eine Beziehung zu mehr als einem Acquirer?

Ja Nein

Teil 2c. Qualifikation zum Ausfüllen von SBF A

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

<input type="checkbox"/>	Der Händler speichert, verarbeitet oder überträgt keine Karteninhaberdaten vor Ort bei sich, sondern verlässt sich ganz auf einen oder mehrere Drittdienstanbieter, der/die diese Funktionen übernimmt/übernehmen.
<input type="checkbox"/>	Es wurde bestätigt, dass die Handhabung, Speicherung, Verarbeitung bzw. Übertragung der Karteninhaberdaten durch den Drittdienstanbieter den PCI-DSS erfüllt.
<input type="checkbox"/>	Der Händler speichert keine Karteninhaberdaten in elektronischem Format und
<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 (*completion date*) notiert wurden, bestätigt (*Merchant Company Name*) folgenden Konformitätsstatus (eine Option auswählen):

<input type="checkbox"/>	Konform: Alle Abschnitte des PCI SBF sind komplett und alle Fragen wurden mit „Ja“ beantwortet, was zu der Gesamtbewertung VOLLE KONFORMITÄT geführt hat, (<i>Merchant Company Name</i>) hat volle Konformität mit dem PCI-DSS demonstriert.
<input type="checkbox"/>	Nicht konform: Nicht alle Abschnitte des PCI SBF sind komplett und einige Fragen wurden mit „Nein“ beantwortet, was zu der Gesamtbewertung KEINE KONFORMITÄT geführt hat, (<i>Merchant Company Name</i>) hat daher nicht die volle Konformität mit dem PCI-DSS demonstriert. <ul style="list-style-type: none"> ▪ Zieldatum für Konformität: ▪ 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>

Teil 3a. Bestätigung des Status „Konform“

Händler bestätigt:

<input type="checkbox"/>	PCI-DSS Selbstbeurteilungs-Fragebogen A, Version (SAQ <i>version #</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 bestätige, dass ich jederzeit meine volle PCI-DSS-Konformität haben muss.

Teil 3b. Bestätigung durch 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 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	
9	Beschränkung des physischen Zugriff auf Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
12	Befolgung einer Informationssicherheits-Richtlinie	<input type="checkbox"/>	<input type="checkbox"/>	

Selbstbeurteilungs-Fragebogen A

Ausfülldatum:

Implementierung starker Zugriffskontrollmaßnahmen

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 Querschnitt-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.

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>
12.8	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 Kompensationskontrolle, wenn (1) die Absicht der ursprünglichen Anforderung erfüllt wird (das Risiko des Abfangens unverschlüsselter Kennwörter wird verhindert) und (2) die Authentifizierung in einer sicheren Umgebung ordnungsgemäß konfiguriert wurde.

- c) Die vorhandenen PCI-DSS-Anforderungen können mit neuen Kontrollen zusammen als Kompensationskontrolle fungieren. Beispiel: Ein Unternehmen kann Karteninhaberdaten nicht nach Anforderung 3.4 unlesbar machen (z. B. durch Verschlüsselung). In diesem Fall könnte eine Kompensation darin bestehen, dass mit einem Gerät bzw. einer Kombination aus Geräten, Anwendungen und Kontrollen folgende Punkte sichergestellt sind: (1) interne Netzwerksegmentierung; (2) Filtern von IP- oder MAC-Adressen und (3) Zwei-Faktor-Authentifizierung innerhalb des internen Netzwerks.
- 4. Sie müssen dem zusätzlichen Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht, angemessen sein.

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

Anhang C: Arbeitsblatt 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 – 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 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>

