INFORMATIONSERGÄNZUNG

# PCI DSS v4.x: Leitfaden für kompensierende Kontrollen und den kundenspezifischen Ansatz

Version: 1.0
Datum: Juni 2026
Autor: PCI Security Standards Council

# Dokumentänderungen

| Datum | Version | Beschreibung |
|---|---|---|
| Juni 2026 | 1.0 | Erste Veröffentlichung |

*ANMERKUNG: Die englische textversion dieses dokuments wie auf der PCI SSC-website angezeigt gilt für alle zwecke als offizielle version dieses dokuments. Für den fall von mehrdeutigkeit oder unstimmigkeit zwischen diesem und dem englischen text hat die englische version vorrang.*

# Inhalt

# Überblick

Der Payment Card Industry Data Security Standard (PCI DSS) ermöglicht Flexibilität bei der Umsetzung der Sicherheitsziele. PCI DSS v4.x umfasst zwei Ansätze für die Implementierung und Validierung der PCI-DSS-Kontrollen vor: den definierten Ansatz und den kundenspezifischen Ansatz. Diese beiden Ansätze unterscheiden sich hinsichtlich ihrer Zielsetzung, ihrer Elemente, ihrer Dokumentation und ihrer Validierung.

Dieses Dokument hebt jeden Ansatz hervor, und:

- Adressiert die Rolle der bewerteten Entitäten
- Adressiert die Rolle der zugeordneten Bewerter und
- Stellt Dokumentation zu diesen Ansätzen und Antworten auf häufig gestellte Fragen bereit.

Für zu bewertende Entitäten enthält dieses Dokument abgeschlossene Beispiele für:

- Arbeitsblatt für Kompensierende Kontrollen,
- Eine Kontrollmatrix für einen kundenspezifischen Ansatz und
- Eine gezielte Risikoanalyse für den kundenspezifischen Ansatz.

Für Bewerter enthält dieses Dokument ein ausgefülltes Beispiel für einen Konformitätsbericht – Anhang E: Vorlage für einen kundenspezifischen Ansatz.

## Zielgruppe und Zweck

Dieses Dokument ist für alle Entitäten bestimmt, die Kontrollen oder einen kundenspezifischen Ansatz entwickeln, betreiben, verwalten oder bewerten. Dazu gehören Bewerter, die PCI-DSS-Bewertungen durchführen und Entitäten, die sich solchen Bewertungen unterziehen.

Der Zweck dieses Dokuments ist es, praktische Leitlinien bereitzustellen, um die einheitliche Anwendung von kompensierenden Kontrollen und des kundenspezifischen Ansatzes zu unterstützen.

Der PCI Security Standards Council (PCI SSC) ist nicht dafür verantwortlich, die Einhaltung der Standards durchzusetzen oder zu bestimmen, ob eine bestimmte Implementierung konform ist. Entitäten sollten mit der/den Organisation(en) zusammenarbeiten, die ihr Konformität-Programm verwalten, wie einem Erwerber (Handelsbank), einer Zahlungsmarke oder einer andere Entität, um die Konformitätsvalidierung und die Berichtspflichten der Entität zu verstehen.

Die in diesem Dokument enthaltenen Leitlinien ergänzen, erweitern, ersetzen oder heben die Anforderungen des PCI DSS oder anderer PCI-SSC-Standards nicht auf. Zum Zeitpunkt der Veröffentlichung ist die aktuelle Version des PCI DSS v4.0.1; die hier dargelegten allgemeinen Grundsätze und Vorgehensweisen können jedoch auch für zukünftige Versionen gelten.

# Optionen zur Implementierung und Validierung der PCI DSS v4.x-Kontrollen

PCI DSS v4.x bietet einer Entität zwei Möglichkeiten, um die PCI-DSS-Anforderungen zu implementieren und zu validieren – den definierten Ansatz und den kundenspezifischen Ansatz.

**Der definierte Ansatz** ist die traditionelle Methode zur Implementierung und Validierung von PCI-DSS-Kontrollen, die bereits seit der ersten Version des PCI-DSS angewendet wird. **Kompensierende Kontrollen sind im Rahmen des definierten Ansatzes** eine Option für Entitäten, die aufgrund einer berechtigten und dokumentierten technischen oder geschäftlichen Einschränkung nicht in der Lage sind, die Anforderungen des definierten Ansatzes wie angegeben zu erfüllen. Kompensierende Kontrollen werden häufig in Situationen verwendet, in denen ein Altsystem oder -prozess vorhanden ist, der nicht an die Anforderungen angepasst werden kann.

**Der kundenspezifische Ansatz** konzentriert sich auf das Sicherheitsziel jeder PCI-DSS-Anforderung (sofern zutreffend) und ermöglicht es Entitäten, Kontrollen zu implementieren, um das in der Anforderung festgelegte Ziel des kundenspezifischen Ansatzes zu erreichen, ohne dabei die definierte Anforderung strikt einzuhalten. Da jede kundenspezifische Implementierung unterschiedlich ist, gibt es keine festgelegten Testverfahren; stattdessen muss der Bewerter Testverfahren ableiten, die der jeweiligen Implementierung angemessen sind, damit er validieren kann, ob die implementierten Kontrollen das festgelegte Ziel erfüllen.

***Ist der kundenspezifische Ansatz eine Option für alle PCI DSS-Anforderungen?***

Die meisten PCI DSS-Anforderungen lassen sich entweder mithilfe des definierten oder des kundenspezifischen Ansatzes erfüllen. Für einige Anforderungen ist jedoch kein Ziel für den kundenspezifischen Ansatz angegeben, sodass keine Option für einen kundenspezifischen Ansatz zur Verfügung steht.

***Für welche Art der Entität ist der kundenspezifische Ansatz gedacht?***

Der kundenspezifische Ansatz soll Innovationen im Bereich der Sicherheitspraktiken fördern und den Entitäten mehr Flexibilität bieten, um nachzuweisen, wie ihre Sicherheitskontrollen die Ziele des PCI DSS erfüllen. Dieser Ansatz wird für risikoreife Entitäten empfohlen, die einen soliden Risikoverwaltungsansatz im Bereich Sicherheit nachweisen können, einschließlich – aber nicht beschränkt auf – einer eigenen Risikomanagementabteilung oder eines entitätsweiten Risikoverwaltungsansatzes.

Es wird erwartet, dass die mithilfe des kundenspezifischen Ansatzes implementierten und validierten Kontrollen das Sicherheitsniveau erreichen oder übertreffen, das durch die Anforderungen des definierten Ansatzes bereitgestellt wird. Daraus folgt, dass der Dokumentationsaufwand und der Aufwand für die Validierung kundenspezifischer Implementierungen ebenfalls größer sein werden als bei dem definierten Ansatz.

***Kann ein kundenspezifischer Ansatz von Entitäten verwendet werden, die einen SAQ ausfüllen?***

Die Verwendung des kundenspezifischen Ansatzes wird in den Selbstbewertungsfragebögen (SAQs) nicht unterstützt. Entitäten, die eine Validierung nach dem kundenspezifischen Ansatz vornehmen möchten, können möglicherweise die PCI-DSS-Vorlage für den Konformitätsbericht (ROC) verwenden, um die Ergebnisse der Bewertung zu dokumentieren. Fragen zur Verwendung des kundenspezifischen Ansatzes, einschließlich der Frage, ob Entitäten, die für einen SAQ in Frage kommen, stattdessen einen ROC ausfüllen können, um einen kundenspezifischen Ansatz zu nutzen, sollten stets an die Organisationen gerichtet werden, die Konformitätsprogramme verwalten, wie zum Beispiel Zahlungsmarken und Erwerber.

Beachten Sie, dass das Ziel des kundenspezifischen Ansatzes einer Anforderung überprüft werden kann, um die Absicht einer Anforderung zu verstehen, selbst wenn eine Entität für diese Anforderung keinen kundenspezifischen Ansatz implementiert.

***Was ist der Unterschied zwischen einer kompensierenden Kontrolle und dem kundenspezifischen Ansatz?***

Es ist wichtig zu beachten, dass kompensierende Kontrollen einen anderen Zweck erfüllen als der kundenspezifische Ansatz. Im Gegensatz zu kompensierenden Kontrollen, die verwendet werden, wenn Organisationen mit Einschränkungen konfrontiert sind und die Anforderung **nicht** wie vorgeschrieben erfüllen können, richtet sich der kundenspezifische Ansatz an Entitäten, die sich dafür entscheiden, die Anforderung auf andere Weise als vorgeschrieben **zu erfüllen**. In diesem Fall muss die Entität das festgelegte Ziel des kundenspezifischen Ansatzes statt der festgelegte Anforderung erfüllen. Der kundenspezifische Ansatz ist dann am erfolgreichsten, wenn die Entität über robuste Sicherheitsprozesse und solide Risikomanagementpraktiken verfügt sowie in der Lage ist, die Dokumentation, das Testen und die Aufrechterhaltung von Sicherheitskontrollen, die diesem Ziel entsprechen, effektiv zu gestalten.

***Kann eine kompensierenden Kontrolle und der kundenspezifische Ansatz für dieselbe Anforderung verwendet werden?***

Ja. Eine Entität kann für bestimmte Systemkomponenten kompensierende Kontrollen und für andere Systemkomponenten den kundenspezifischen Ansatz verwenden, um dieselbe Anforderung zu erfüllen. Am Beispiel der Anforderung 5.3.1 könnte eine Entität eine kompensierende Kontrolle einsetzen, um diese Anforderung für einen bestimmten Servertyp zu erfüllen, wenn eine berechtigte und dokumentierte geschäftliche Einschränkung vorliegt, die verhindert, dass dieser Server die festgelegte Anforderung erfüllt. Die Entität kann sich auch dafür entscheiden, den kundenspezifischen Ansatz zu nutzen, um dieselbe Anforderung für andere Systemkomponenten zu erfüllen, sofern es dort einen eigenen Ansatz zur Erkennung und Bekämpfung der neuesten Malware-Bedrohungen implementiert hat. Die Entität könnte den beschriebenen definierten Ansatz auch nutzen, um dieselbe Anforderung für eine andere Gruppe von Systemkomponenten zu erfüllen.

**Wenn eine Entität einen kundenspezifischen Ansatz entwickelt, der das Ziel des kundenspezifischen Ansatzes nicht erfüllt, kann die Entität dann stattdessen eine kompensierende Kontrolle einsetzen, um das Ziel des kundenspezifischen Ansatzes zu erreichen?**

Nein. Kompensierende Kontrollen sind bei dem kundenspezifischen Ansatz keine Option. Der kundenspezifische Ansatz richtet sich an Organisationen, die sich dafür entscheiden, eigene Kontrollen zu entwickeln, die dem Ziel des kundenspezifischen Ansatzes der Anforderung entsprechen. Wenn eine Organisation einen kundenspezifischen Ansatz entwickelt und anschließend auf technische oder geschäftliche Einschränkungen stößt, die sie daran hindert, das Ziel des kundenspezifischen Ansatzes zu erreichen, bedeutet dies, dass die Organisation einen kundenspezifischen Ansatz konzipiert hat, den sie nicht umsetzen kann. Aus diesem Grund kommen kompensierende Kontrollen bei dem kundenspezifischen Ansatz nicht in Frage.

Wenn eine Entität bestimmt, dass sie eine PCI DSS-Anforderung nicht mit einem kundenspezifischen Ansatz erfüllen kann und dass technische oder geschäftliche Einschränkungen vorliegen, die sie daran hindern, die Anforderung des definierten Ansatzes in seiner ursprünglichen Form zu erfüllen, kann die Entität stattdessen eine kompensierende Kontrolle auf der Grundlage der ursprünglichen Anforderung des definierten Ansatzes implementieren.

# Vergleich von Anwendungsfällen: Beispiele für kompensierende Kontrollen und den kundenspezifischen Ansatz

*Diese Beispiele dienen lediglich dazu, Anwendungsfälle zu unterscheiden, bei denen eine kompensierende Kontrolle oder ein kundenspezifischer Ansatz in Betracht gezogen werden könnte. Diese Anwendungsfälle sollen keine konkreten Implementierungen oder Kontrollen veranschaulichen, die für eine bestimmte Umgebung geeignet sind oder deren Einsatz dort empfohlen wird. Die Entität sollte sich stets mit ihrem Bewerter und der Entität, bei dem sie die Nachweise zur Einhaltung der Vorschriften einreichen wird, über die Zulässigkeit und die Anwendung etwaiger kompensierender oder kundenspezifischer Kontrollen abstimmen.*

<table>
<tr><th>Über eine kompensierende Kontrolle adressiert</th><th>Über einen kundenspezifischen Ansatz adressiert</th></tr>
<tr><td>Anforderung 3.3.1.2<br><br>SAD wird nach der Autorisierung gespeichert, da die Entität nicht über die technischen Mittel verfügt, um die Speicherung zu verhindern.</td><td>Diese Anforderung ist nicht für den kundenspezifischen Ansatz berechtigt.</td></tr>
<tr><td>Anforderung 3.5.1<br><br>Aufgrund einer technischen Einschränkung kann die PAN nicht verschlüsselt oder auf andere Weise unlesbar gemacht werden.</td><td></td></tr>
<tr><td>Anforderung 5.2.1<br><br>Aufgrund technischer Einschränkungen können Anti-Malware-Lösungen auf bestimmten Systemen nicht eingesetzt werden.</td><td>Anforderung 5.2.1<br><br>Es gibt einen Mechanismus, der jegliche Malware erkennt und deren Installation oder Ausführung verhindert.</td></tr>
<tr><td colspan="2">Anforderung 8.3.6<br><br>Das Tool eines Cloud-Anbieters lässt keine Änderungen an den Passwortkonfigurationen zu, und die bereitgestellten Konfigurationen entsprechen nicht den PCI DSS-Anforderungen.<br><br>Dies könnte je nach der implementierten Kontrolle entweder durch eine kompensierende Kontrolle oder einen kundenspezifischen Ansatz gelöst werden.</td></tr>
<tr><td></td><td>Anforderung 11.3.1<br><br>Interne Schwachstellen werden mit einer anderen Methode als dem internen Schwachstellenscan identifiziert.</td></tr>
<tr><td>Anforderung 11.3.2<br><br>Aufgrund einer anstehenden Änderung am ASV-Tool kann der nächste externe Schwachstellenscan nicht termingerecht durchgeführt werden.</td><td>Diese Anforderung ist nicht für den kundenspezifischen Ansatz berechtigt.</td></tr>
<tr><td></td><td>Anforderung 11.5.1<br><br>Zur Erkennung von anomalem Netzwerkverkehr wird ein anderer Mechanismus als IDS/IPS verwendet.</td></tr>
</table>

# Rollen für kompensierende Kontrollen und den kundenspezifischen Ansatz

## Rolle der Entität: Kompensierende Kontrollen

Von den Entitäten wird erwartet, dass sie bei Anwendung von kompensierenden Kontrollen diese definieren und durch Ausfüllen eines oder mehrerer Arbeitsblätter für kompensierende Kontrollen (CCWs) dokumentieren. Die CCWs der Entität sollten Folgendes umfassen:

- Deutlich definierte technische und/oder geschäftliche Einschränkungen, die die Entität daran hindern, die angegebene PCI DSS-Anforderung zu erfüllen.
- Die Definition der kompensierenden Kontrolle und eine Erläuterung, wie die Kontrolle die Ziele der ursprünglichen Anforderung adressiert und etwaige erhöhte Risiken berücksichtigt: beispielsweise in Bezug auf die Personen, Prozesse, Richtlinien und/oder Technologien, aus denen sich die Kontrolle zusammensetzt.
- Das Ziel der ursprünglichen Kontrolle:
  - Die Entität kann für dieses Ziel das Ziel des kundenspezifischen Ansatzes der Anforderung verwenden, sie ist jedoch nicht dazu verpflichtet.
- Das durch die kompensierende Kontrolle erreichte Ziel:
  - Dies kann, muss aber nicht unbedingt das für diese Anforderung in der PCI DSS-Anforderung angegebene Ziel des kundenspezifischen Ansatzes sein.
- Eine Beschreibung von zusätzlichen Risiken, die sich aus dem Fehlen der ursprünglichen Kontrollen ergeben. Die Dokumentation sollte ein Verständnis für dieses Risiko und die Art und Weise, wie ihm begegnet wird, widerspiegeln.
- Eine Erläuterung, wie die Entität die kompensierende Kontrolle validiert und testet.
- Eine Definition der Prozesse und Kontrollen, die die Entität zur Aufrechterhaltung der kompensierenden Kontrolle eingeführt hat.

Ein Muster für ein CCW ist in *Anhang C* des PCI DSS v4.x enthalten: *Arbeitsblatt für Kompensierende Kontrollen.* Eine Vorlage für ein *Arbeitsblatt zur zusätzlichen Kompensationskontrolle* ist auf der PCI SSC-Webseite in der Dokumentenbibliothek unter „PCI DSS“ verfügbar.

## Rolle des Bewerters: Kompensierende Kontrollen

Die Bewerter sind verpflichtet, die „Compensating Controls Worksheets“ (CCW) der Entität bei jeder jährlichen PCI-DSS-Bewertung gründlich zu bewerten, um sicherzustellen, dass die CCW die in Anhang C adressierten Punkte klar und wirksam dokumentieren und berücksichtigen: *Arbeitsblatt für Kompensierende Kontrollen*, siehe oben unter „Rolle der Entität“.

Im Falle einer von der Entität dokumentierten berechtigten technischen oder geschäftlichen Einschränkung wird vom Bewerter nicht erwartet, dass er die Gültigkeit dieser geschäftlichen oder technischen Einschränkung bestätigt, sondern lediglich, dass die Einschränkung von der Entität umfassend dokumentiert ist. Vom Bewerter wird jedoch erwartet, dass er die von der Entität implementierten Kontrollelemente prüft, um sich zu vergewissern, dass die kompensierende Kontrolle vorhanden ist und wirksam funktioniert.

Vom Bewerter wird erwartet, dass:

- Fügen Sie die CCWs der Entität gegebenenfalls in den Konformitätsbericht (ROC) oder den Selbstbewertungsfragebogen (SAQ) ein.
- Führen Sie Tests der kompensierenden Kontrollen durch, einschließlich der Prüfung von Konfigurationseinstellungen, der Prüfung von Dokumentationen, der Beobachtung von Prozessen usw., soweit dies für die jeweilige Anforderung und die zu prüfende Kontrollmaßnahme relevant ist.
  - Die Testverfahren der Anforderung können als Leitfaden für die Art der zu erwartenden Tests für diese Anforderung angesehen werden.
- Beim Ausfüllen eines ROC ist für jede PCI-DSS-Anforderung, die durch eine kompensierende Kontrolle erfüllt wird, Folgendes anzugeben:
  - Aktivieren Sie das Kontrollkästchen „kompensierende Kontrolle“.
  - Fügen Sie eine Beschreibung hinzu, wie die Prüfungen und Nachweise des Bewerters belegen, dass die Anforderung erfüllt ist.
  - Die durchgeführten Prüfungen sind in den Arbeitsunterlagen des Bewerters zu dokumentieren und die Nachweise zusammen mit den übrigen Prüfungsnachweisen aufzubewahren.

***Kann eine kompensierende Kontrolle eingesetzt werden, um eine in der Vergangenheit versäumte Anforderung zu erfüllen?***

Nein. Für PCI DSS v4.x, Anhang B: Die Kompensierenden Kontrollen wurden aktualisiert, um klarzustellen, dass *kompensierende Kontrollen nicht dazu verwendet werden können, eine in der Vergangenheit versäumte Anforderung rückwirkend zu beheben.* Es war nie die Absicht, dass kompensierende Kontrollen auf diese Weise eingesetzt werden könnten. Beispielsweise wurde eine Aufgabe, die hätte erledigt werden sollen, nicht erledigt, und es wurden zu diesem Zeitpunkt keine Maßnahmen ergriffen, um dem entgegenzuwirken. Eine Entität kann jedoch eine kompensierende Kontrolle implementieren, um Faktoren zu berücksichtigen, die sich auf die künftige Ausführung einer Aufgabe auswirken könnten (beispielsweise um geplante Systemausfälle oder Urlaubstage von Mitarbeitern vorwegzunehmen).

***Kann eine kompensierende Kontrolle zur Erfüllung mehrerer PCI-DSS-Anforderungen eingesetzt werden?***

Ja. Eine kompensierende Kontrolle kann entwickelt werden, um das Risiko zu mindern, dass mehr als eine Anforderung nicht erfüllt wird. Wie jedoch jede Anforderung durch die jeweilige kompensierende Kontrolle erfüllt wird, muss separat in einzelnen kompensierende Kontroll-Arbeitsblättern dokumentiert werden.

Alle mit jeder Anforderung verbundenen Ziele und Risiken müssen berücksichtigt werden, und die kompensierende Kontrolle muss für jede Anforderung unabhängig validiert werden.

**Muss eine kompensierende Kontrolle nur für eine begrenzte Dauer eingesetzt werden?**

Nein. Es gibt keine Vorschrift, wonach eine Ausgleichskontrolle nur für einen begrenzten Zeitraum bestehen darf; die geprüfte Entität sollte ihre kompensierenden Kontrollen jedoch jährlich überprüfen, um sicherzustellen, dass diese weiterhin wirksam und notwendig sind. Beispielsweise kann eine neue Technologie oder ein neues System eine überarbeitete kompensierende Kontrolle erfordern, um das Ziel der Anforderung zu erreichen, oder es kann die Notwendigkeit einer kompensierende Kontrolle außer Kraft gesetzt haben, sodass die ursprüngliche PCI DSS-Anforderung nun wie angegeben erfüllt werden kann.

Ebenso wird vom Bewerter erwartet, dass er die kompensierenden Kontrollen der Entität jährlich überprüft, um sicherzustellen, dass diese nach wie vor angemessen und notwendig sind, um das Risiko zu bewältigen und die Anforderung zu erfüllen.

# Rolle der Entität: Kundenspezifischer Ansatz

Die bewertete Entität entwirft, entwickelt, analysiert, implementiert und pflegt ihre kundenspezifischen Kontrollen, wobei sie die folgenden Schritte durchführt:

- Überprüfen Sie die Informationen zum kundenspezifischen Ansatz im Abschnitt Referenzen und Begleitmaterialien dieses Dokuments.
- Definieren und dokumentieren Sie jede kundenspezifische Kontrolle, einschließlich einer Beschreibung, wie die Kontrolle das Ziel der Anforderung erfüllt. Siehe die *Beispielhafte Kontrollmatrixvorlage*[1] für eine Vorlage, die verwendet werden kann, um Informationen über die kundenspezifische Kontrolle zu dokumentieren.
- Führen Sie eine gezielte Risikoanalyse durch und dokumentieren Sie diese, die zeigt, dass die kundenspezifische Kontrollmaßnahme ausreichend robust ist, um mindestens den gleichen Schutz wie die definierte Anforderung zu gewährleisten. Siehe die *Beispielhafte gezielte Risikoanalysevorlage*[1] für eine Vorlage, die verwendet werden kann, um Informationen über die kundenspezifische Kontrolle zu dokumentieren.
- Führen Sie Tests durch und dokumentieren Sie diese, um zu bestätigen, dass jede kundenspezifische Kontrolle das Ziel der Anforderung wirksam erfüllt. Siehe Sie die *Beispielhafte Kontrollmatrixvorlage,* um die durchgeführten Tests und die Testergebnisse zu dokumentieren.
- Beschreiben Sie, wie die Wirksamkeit der einzelnen Kontrollen im Laufe der Zeit überwacht und aufrechterhalten wird.
- Sprechen Sie frühzeitig mit Ihrem Bewerter über Pläne zur Implementierung eines kundenspezifischen Ansatzes.
- Bitte legen Sie Ihrem Bewerter sämtliche Unterlagen zu jeder kundenspezifischen Kontrolle vor.

Damit die bewertete Entität ihre kundenspezifischen Kontrollen wirksam implementieren und aufrechterhalten kann, ist es wichtig, dass die Entität diese kundenspezifischen Kontrollen verinnerlicht und sich aktiv dafür einsetzt.

# Rolle des Bewerters: Kundenspezifischer Ansatz

Bei Anwendung des kundenspezifischen Ansatzes sollten die Bewerter davon ausgehen, dass sie die Dokumentation der Entität zu diesem Ansatz im Voraus erhalten, um sie bei der Durchführung der folgenden Schritte zu unterstützen:

- Bestätigen sie, ob die betreffende PCI-DSS-Anforderung für den kundenspezifischen Ansatz geeignet ist.
- Überprüfen Sie die Dokumentation der Entität, um die kundenspezifisch Kontrolle vollständig zu verstehen.
  - Bestätigen Sie, dass sowohl eine Kontrollmatrix als auch eine gezielte Risikoanalyse erstellt und bereitgestellt wurden.

[1] Die Beispielvorlagen enthalten zwei Vorlagen: Kundenspezifischer Ansatz – 1) Kundenspezifischer Ansatz – Beispielhafte Kontrollmatrixvorlage und 2) Kundenspezifischer Ansatz – Beispielhafte gezielte Risikoanalysevorlage. Dieses Dokument ist auf der Webseite des PCI SSC in der Dokumentenbibliothek unter PCI DSS verfügbar. Zwar sind Entitäten nicht verpflichtet, die spezifischen Formate dieser Vorlagen einzuhalten, doch müssen die „Customized Approach Controls Matrix“ und die „Targeted Risk Analysis“ der Entität alle in diesen Vorlagen enthaltenen Informationen umfassen, wie in Anforderung 12.3.2 des PCI DSS festgelegt.

- Bestätigen Sie, dass jede kundenspezifische Kontrolle ausreichend dokumentiert ist, einschließlich der folgenden Punkte:
  - Die Dokumentation enthält alle erforderlichen Informationen gemäß den Vorlagen für die kundenspezifischen Ansatz-Kontrollmatrix und die gezielte Risikoanalyse.
  - In der Dokumentation wird beschrieben, wie die kundenspezifische Kontrolle mindestens den gleichen Schutz bietet wie die definierte Anforderung.
- Prüfen Sie die von der Entität durchgeführten Tests der kundenspezifischen Kontrolle sowie die Testergebnisse, um zu bestimmen, ob die von der Entität durchgeführten Tests ausreichten, um die Kontrollen gründlich zu bewerten.
- Leiten Sie robuste Testverfahren ab, die eine gründliche Prüfung jeder kundenspezifischen Kontrolle ergeben.
  - Die von der Entität vorgelegte Dokumentation muss so detailliert sein, dass der Bewerter die Funktionsweise der Kontrolle nachvollziehen und daraus geeignete Prüfverfahren ableiten kann.
  - Wenn der Bewerter feststellt, dass die von der Entität durchgeführten Tests eine gründliche Bewertung der Kontrolle ermöglichten, kann er optional auf die Tests der Entität zurückgreifen, um seine eigenen Prüfungen der Wirksamkeit der Kontrolle durchzuführen. In diesem Fall sollte der Bewerter ein anderes Beispiel verwenden als das, das von der Entität herangezogen wurde.
- Führen Sie unabhängige Tests für jede kundenspezifische Kontrollimplementierung durch. Verlassen Sie sich nicht ausschließlich auf die Ergebnisse der von der Entität durchgeführten Tests. Die Absicht des Testens durch den Bewerter ist es festzustellen, ob die Kontrolle:
  - Die Anforderungen hinsichtlich des kundenspezifischen Ansatzes erfüllt,
  - Aufrechterhalten wird, um die fortlaufende Wirksamkeit zu gewährleisten, und
  - Ausreichend ist, um zu dem Ergebnis „Vorhanden“ zu gelangen.
- Dokumentieren Sie jede kundenspezifische Kontrolle im Konformitätsbericht (ROC), sowohl bei der Anforderung als auch im ROC-*Anhang E: Kundenspezifische Ansatzvorlage*:
  - Während einer Bewertung füllt der Prüfer diesen Anhang für jeden Fall aus, in dem eine kundenspezifische Kontrolle verwendet wird, um eine PCIDSS-Anforderung zu erfüllen.
  - Neben den Informationen über die kundenspezifische Kontrolle aus der Dokumentation der Entität wird vom Bewerter erwartet, dass er Einzelheiten zu den von ihm entwickelten Testverfahren, zu den von ihm geprüften Nachweisen, die bestätigen, dass die Kontrolle vorhanden ist und wirksam funktioniert, sowie zu den Ergebnissen der von ihm durchgeführten Prüfungen angibt.

**Kann bei dem kundenspezifischen Ansatz der von der Entität durchgeführte Test den Test durch den Bewerter ersetzen?**

Nein. Die von der Entität durchgeführten Tests sind im Rahmen der Implementierung und der Aufrechterhaltung ihres kundenspezifischen Ansatzes erforderlich, um die Wirksamkeit der Kontrollen nachzuweisen, ersetzen jedoch nicht die vom Bewerter durchgeführten Tests. Der Bewerter muss unabhängige Tests durchführen und seine Schlussfolgerungen zur Bewertervalidierung auf den Ergebnissen dieser Tests basieren. Wenn der Bewerter festgestellt hat, dass die von der Entität durchgeführten Tests eine gründliche Bewertung der Kontrolle ermöglichten, kann er denselben Test verwenden, jedoch mit einer anderen Stichprobe als die von der Entität verwendete.

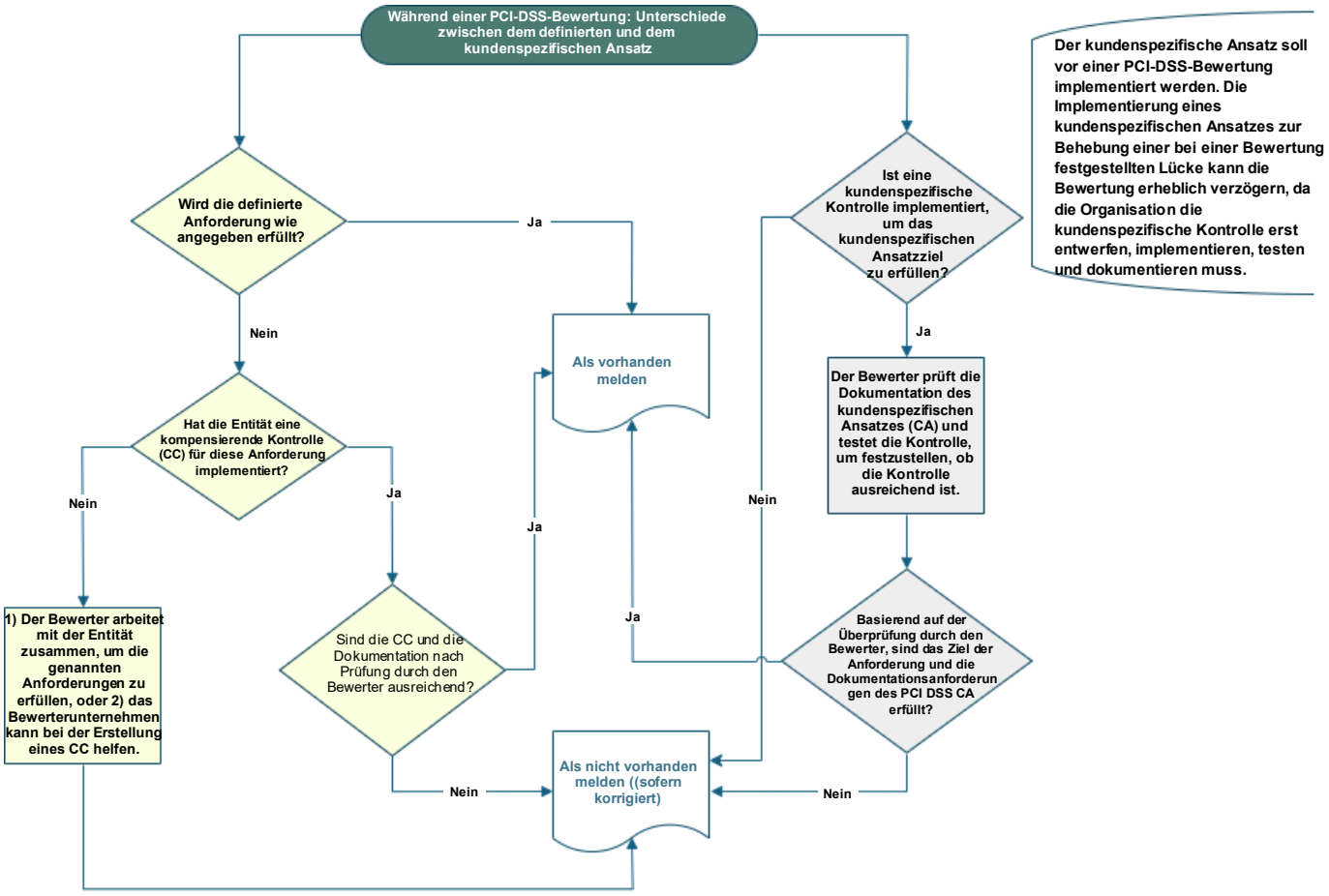
***Warum ist für einen kundenspezifischen Ansatz mehr Dokumentation erforderlich als für eine kompensierende Kontrolle?***

Kundenspezifische Implementierungen variieren je nach Konzeption und Umgebung und werden vollständig von der bewerteten Entität selbst konzipiert. Da die Kontrolle von der Entität selbst entworfen wird und daher im PCI DSS nicht definiert ist, gibt es auch keine vordefinierten Testverfahren. Aus diesem Grund ist es unerlässlich, dass die Dokumentation der Entität umfassend ist – sie muss definieren, worin die Kontrolle besteht, wie sie implementiert wird, welches Risiko besteht, wie dieses Risiko angegangen wird, wie die Kontrolle von der Entität getestet wird, inwiefern die Kontrolle das festgelegte Ziel erfüllt, wie die Entität die Gewissheit erlangt, dass die Kontrolle dauerhaft wirksam ist, usw.

Diese Dokumentation ermöglicht es dem Bewerter, die Kontrolle und ihre Funktionsweise vollständig zu verstehen, sodass er geeignete Testverfahren ableiten und die Kontrolle unabhängig validieren kann.

Das nachstehende Diagramm veranschaulicht die Unterschiede zwischen dem Ansatz zu kompensierenden Kontrollen und dem kundenspezifischen Ansatz bei einer PCI-DSS-Bewertung.

## Figur 1: Wie sich der definierte Ansatz und der kundenspezifische Ansatz bei einer PCI DSS-Bewertung unterscheiden



# Dokumentierung von kompensierenden Kontrollen und den kundenspezifischen Ansatz

Entitäten werden dazu angehalten, eine klare, vollständige und gut strukturierte Dokumentation ihrer kompensierenden oder kundenspezifischen Kontrollen zu erstellen. Eine gründliche Dokumentation stellt den Bewertern eine solide Grundlage bereit, um die Kontrolle, die Umgebung und die Art und Weise, wie die Kontrolle den Zweck der PCI-DSS-Anforderung oder des PCI-DSS-Ziels erfüllt, zu verstehen und zu bewerten.

Die Qualität der Dokumentation der Entität wirkt sich unmittelbar auf die Fähigkeit eines Bewerters aus, die Kontrollen zu validieren und zu einer vertretbaren Schlussfolgerung zu gelangen.

Sowohl bei kompensierenden Kontrollen als auch bei kundenspezifischen Implementierungen sollte die Dokumentation der Entität:

- Vollständig, klar und für einen selbstständigen Leser verständlich sein.
- Für sich alleinstehen, ohne auf undokumentierten Kontext angewiesen zu sein.
- Klar aufzeigen, wie die Ziele erreicht und die Risiken bewältigt werden.
- Nachweise darüber enthalten, wie die Entität sichergestellt hat, dass die Kontrolle wirksam funktioniert, einschließlich Einzelheiten zu den Prozessen und Ergebnissen der Entität im Hinblick auf Validierung, Prüfung und laufende Überwachung.

***Kann eine kompensierende Kontrolle oder ein kundenspezifischer Ansatz validiert werden, wenn die Dokumentation oder die Nachweise der Entität unvollständig sind?***

Nein. Wenn die Dokumentation nicht ausreicht, kann der Bewerter möglicherweise nicht bestätigen, dass die Kontrolle effektiv konzipiert ist und funktioniert. Wenn die Entität dem Bewerter keine ausreichenden Nachweise bereitstellt oder wenn der Bewerter keine Gewissheit darüber hat, dass die Dokumentation und die Kontrollen der Entität ausreichend sind, kann der Bewerter entscheiden, ob die Feststellung „Nicht vorhanden“ das angemessene Ergebnis ist.

# Unabhängigkeit des Bewerters

Die Unabhängigkeit des Bewerters ist ein Grundprinzip der PCI DSS-Bewertungen und gilt gleichermaßen für die Validierung von kompensierenden Kontrollen und kundenspezifischen Implementierungen. Die bewertete Entität ist für die Entwicklung, Implementierung und Aufrechterhaltung von kompensierenden Kontrollen verantwortlich.

**Können QSAs im Auftrag einer Organisation Kontrollen entwerfen oder implementieren?**

Zwar dürfen QSA-Mitarbeiter Entitäten bei dem Design oder der Implementierung von Kontrollen unterstützen, aber QSA- Unternehmen müssen die in der *QSA Qualifizierter Sicherheitsbewerter* und *QSA Programmleitfaden* Unabhängigkeitsanforderungen einhalten. Dies beinhaltet die Einrichtung von Kontrollen zur Trennung der Aufgaben, um sicherzustellen, dass die QSA-Mitarbeiter, die eine PCI DSS-Bewertung durchführen oder dabei mitwirken, unabhängig sind und keinem Interessenkonflikt unterliegen.

Es wäre ein Interessenkonflikt, wenn ein QSA-Mitarbeiter, der an der Konzeption oder Implementierung einer Kontrolle beteiligt war, auch eine kompensierende oder kundenspezifische Kontrolle testen, bewerten oder bei deren Bewertung mitwirken würde. Siehe *FAQ 1562*, „Darf ein QSA-Mitarbeiter, der spezifische Kontrollen für einen Kunden entwirft, entwickelt oder implementiert, auch diese Kontrollen bewerten?“ Weitere Informationen finden Sie auf der FAQ-Seite des PCI SSC.

**Speziell für den kundenspezifischen Ansatz**

Ein QSA-Mitarbeiter kann zwar Beratungsleistungen im Zusammenhang mit dem kundenspezifischen Ansatz erbringen, aber eine Organisation, die einen QSA benötigt, um ihre kundenspezifischen Kontrollen zu entwerfen oder zu implementieren, ist möglicherweise kein guter Kandidat für den kundenspezifischen Ansatz, da es für die Organisation schwierig sein könnte, diese Kontrolle aufrechtzuerhalten und sicherzustellen, dass sie weiterhin effektiv funktioniert. Eine Organisation, die über Risikoreife, Engagement und die notwendigen Ressourcen verfügt, um ihre eigenen kundenspezifischen Kontrollen zu entwickeln, zu implementieren und aufrechtzuerhalten, wird mit größerer Wahrscheinlichkeit eine langfristige Sicherheitseffektivität mit kundenspezifischen Kontrollen erreichen.

Jegliche Beteiligung eines Bewerters oder eines QSA-Unternehmens an der Entwicklung von kompensierenden oder kundenspezifischen Kontrollen muss in Abschnitt 1.4 des Konformitätsberichts (ROC) dokumentiert werden.

# Referenzen und Begleitmaterialien

Beachten Sie die folgenden Abschnitte und Anhänge des PCI DSS v4.x sowie die folgenden Leitfäden, Vorlagen und Formulare:

**Für den kundenspezifischen Ansatz**

- PCI DSS v4.x Einleitungsabschnitt 8 vergleicht kompensierende Kontrollen und den kundenspezifischen Ansatz und gibt einen Überblick über beide Ansätze.
- PCI DSS v4.x Anhang D enthält weitere Einzelheiten zu diesem kundenspezifischen Ansatz, einschließlich der Elemente der erforderlichen gezielten Risikoanalyse und der Verantwortlichkeiten sowohl der Entität als auch des Bewerters.
- In PCI DSS v4.x, *Figur 5 Verständnis der Bestandteile der Anforderungen* zeigt die Position der definierten Ansatz innerhalb jeder Anforderung und, falls zutreffend, des kundenspezifischen Ansatzziels.
- Anforderung 12.3.2 definiert für eine gezielte Risikoanalyse (TRA) für jede PCI DSS-Anforderung, die mit einem kundenspezifischen Ansatz erfüllt wird, die Elemente einer TRA für einen kundenspezifischen Ansatz.
- Vorlage für den PCI DSS 4.x-Konformitätsbericht, Anhang E Vorlage für einen kundenspezifischen Ansatz.
- *Beispielvorlagen: Der kundenspezifische Ansatz* ist auf der PCI SSC-Website in der Dokumentenbibliothek unter PCI DSS verfügbar. Dieses Dokument enthält Folgendes:
  - Kundenspezifischer Ansatz – Beispielhafte Kontrollmatrixvorlage
  - Kundenspezifischer Ansatz – Beispielhafte gezielte Risikoanalysevorlage
- *PCI DSS v4.x: Leitfaden zur gezielten Risikoanalyse* – Beschreibt die zwei verschiedenen Arten von gezielten Risikoanalysen (TRAs), die in PCI DSS v4.x enthalten sind.

**Für kompensierende Kontrollen**

- Innerhalb PCI DSS v4.x:
  - Einleitender Abschnitt 8, in dem kompensierende Kontrollen Regelungen und der kundenspezifische Ansatz verglichen werden und ein Überblick über beide Ansätze gegeben wird.
  - *Anhang B:* Kompensierende Kontrollen, die die Definition und die grundlegenden Kriterien liefern.
  - *Anhang C: Arbeitsblatt kompensierende Kontrollen* – ein Muster des Arbeitsblatts, das Entitäten zur Definition von kompensierenden verwenden, wenn diese zur Erfüllung einer PCI DSS-Anforderung eingesetzt werden.
- Ein *Arbeitsblatt Zusätzliche kompensierende Kontrollen*, das Entitäten zur Dokumentation kompensierender Kontrollen verwenden können, ist auf der Webseite des PCI SSC in der Dokumentenbibliothek unter „PCI DSS“ verfügbar.

# Anhang: Beispiele für ausgefüllte kompensierende Kontroll- und kundenspezifische Ansatzvorlagen

## Ausgefülltes Beispiel für eine Entität: Arbeitsblatt zu kompensierenden Kontrollen

*Beachten Sie, dass dies lediglich als Beispiel für eine Möglichkeit zur Erstellung des Arbeitsblatt zu kompensierenden Kontrollen dient und nicht als Beispiel für eine konkrete Kontrolle gedacht ist, die für eine bestimmte Umgebung geeignet oder deren Einsatz dort empfohlen wird.*

**Anforderungsnummer und Definition:** PCI DSS Anforderung 8.4.2 – Für alle Zugriffe auf die Karteninhaberdatenumgebung (CDE) wird eine Multi-Faktor-Authentifizierung (MFA) implementiert.

| | Erforderliche Informationen | Erläuterung |
|---|---|---|
| **1. Einschränkungen** | Dokumentieren Sie die legitimen technischen oder geschäftlichen Einschränkungen, die die Einhaltung der ursprünglichen Anforderung ausschließen. | ABC Org betreibt eine veraltete Zahlungsautorisierungsplattform (System-ID: PCIPAY-AUTH-01), die auf der proprietären UNIX-Version 5.2 läuft. Diese Plattform unterstützt keine Integration mit modernen MFA-Mechanismen, einschließlich RADIUS-, SAML- oder PAM-basierter MFA-Module. Die Plattform wird vom Hersteller unterstützt, kann aber nicht verändert werden, ohne die Unterstützung durch den Hersteller und die Systemintegrität zu beeinträchtigen.<br><br>Die Erneuerung dieses Systems ist im Rahmen des Projekts PCIPAY-MODERN-02 geplant; die Fertigstellung ist für das vierte Quartal 2027 vorgesehen. |
| **2. Definition von kompensierenden Kontrollen** | Definieren Sie die kompensierenden Kontrollen: erläutern Sie, wie diese die Ziele der ursprünglichen Kontrolle und das gegebenenfalls erhöhte Risiko berücksichtigen. | ABC-Org hat folgende kompensierende Kontrollen implementiert:<br><br>**Jump Host MFA-Durchsetzung**<br><br>Der Zugriff auf PAY-AUTH-01 ist ausschließlich dedizierten administrativen Jump-Hosts innerhalb des Netzwerksegments VLAN-SEC-ADM vorbehalten.<br><br>Der Zugriff auf Jump-Hosts erfordert Folgendes:<br>▪ Eindeutige Benutzer-ID<br>▪ Passwortauthentifizierung<br>▪ Hardwarebasiertes Authentifizierungstoken (FIPS-validiertes Gerät)<br>▪ Active Directory-Authentifizierungsintegration<br><br>**Netzwerkzugriffskontrollen**<br><br>Firewallregeln beschränken den Zugriff auf PAY-AUTH-01 ausschließlich von Jump-Hosts aus. Der direkte Zugriff von Benutzerarbeitsplätzen, VPN-Verbindungen oder anderen Netzwerksegmenten wird technisch verhindert. Firewall-Regelsatzreferenz: FW-RULE-SET-CDE-ADM-V3. |

| | Erforderliche Informationen | Erläuterung |
|---|---|---|
| | | **Sitzungsüberwachung und Protokollierung**<br><br>Alle administrativen Sitzungen werden:<br>▪ Zentral protokolliert<br>▪ An die Enterprise-SIEM-Plattform (SecurityLog-SIEM-01) weitergeleitet<br>▪ Mindestens 12 Monate aufbewahrt<br><br>**Sitzungsaufzeichnung**<br><br>Administrative Sitzungen zu PAY-AUTH-01 werden mithilfe der privilegierten Zugriffsverwaltungs(PAM)-Lösung PAM-SEC-01 protokolliert. Die Sitzungsaufzeichnungen werden zu forensischen und Überwachungszwecken aufbewahrt.<br><br>**Sicherheitsüberwachung und Warnmeldung**<br><br>Das SIEM generiert Warnmeldungen für:<br>▪ Nicht autorisierte Zugriffsversuche<br>▪ Zugriff außerhalb definierter Verwaltungszeitfenster<br>▪ Versuche, Berechtigungen zu erweitern<br><br>Die Warnmeldungen werden von den Mitarbeitern des SOC geprüft. |
| **3. Ziel** | Definieren Sie das Ziel der ursprünglichen Kontrolle. | Um eine starke Authentifizierung für den Zugriff auf das CDE durch die Verwendung mehrerer Authentifizierungsfaktoren zu gewährleisten. |
| | Identifizieren Sie das Ziel, das durch die kompensierende Kontrolle erreicht wird.<br><br>***Hinweis:*** Dies kann, muss aber nicht unbedingt das für diese Anforderung im PCI DSS angegebene Ziel des kundenspezifischen Ansatzes sein. | Die kompensierende Kontrolle erreicht das Ziel der Anforderung, indem sie vor der Gewährung des Zugriffs auf PCIPAY-AUTH-01 eine Multi-Faktor-Authentifizierung (MFA) erzwingt und den direkten Zugriff auf das System verhindert. |
| **4. Identifiziertes Risiko** | Identifizieren Sie zusätzliche Risiken, die sich aus dem Fehlen der ursprünglichen Kontrollen ergeben. | Zu den Risiken, die mit der Unfähigkeit verbunden sind, MFA direkt auf PCIPAY-AUTH-01 zu implementieren, gehören:<br>▪ Potentielle Kompromittierung von Authentifizierungsdaten<br>▪ Nicht autorisierter Zugriff auf Karteninhaberdatensysteme<br><br>Die implementierten kompensierenden Kontrollen mindern dieses Risiko, indem sie Folgendes sicherstellen:<br>▪ Vor dem Zugriff wird eine MFA-Authentifizierung erzwungen<br>▪ Der direkte Zugriff wird verhindert<br>▪ Jeder Zugriff wird überwacht, protokolliert und überprüft<br><br>Das Restrisiko wird als gering eingestuft. |

| | Erforderliche Informationen | Erläuterung |
|---|---|---|
| **5. Validierung von kompensierenden Kontrollen** | Definieren Sie, wie die kompensierenden Kontrollen validiert und getestet wurden. | Die Entität validiert die Wirksamkeit der kompensierenden Kontrolle durch:<br>▪ Vierteljährliche Überprüfung der Firewall-Regeln (Nachweis: (FW-Überprüfung-Berichte)<br>▪ Vierteljährliche Überprüfungen des privilegierten Zugriffs (Nachweis: Zugriff-Überprüfung-Datensätze)<br>▪ Vierteljährliche Verifizierung der Durchsetzung der MFA auf Jump-Hosts<br>▪ Monatliche Verifizierung der SIEM-Warnmeldungen<br>▪ Jährliche interne Prüfung der Kontrollen für privilegierten Zugriff<br><br>Die Entität hat diese Validierungsnachweise geprüft, um sich zu vergewissern, dass die Kontrolle wirksam ist:<br>▪ Firewall-Konfigurationen<br>▪ Konfigurationen der Zugriffskontrolle<br>▪ SIEM-Alarmberichte<br>▪ Sitzungsaufzeichnungsprotokolle |
| **6. Aufrechterhaltung** | Definieren Sie die Prozesse und bestehenden Kontrollen zur Aufrechterhaltung der kompensierenden Kontrollen. | Die Entität gewährleistet die Wirksamkeit der kompensierenden Kontrollen durch:<br>▪ Verfahren zur Änderungsvewaltung für Konfigurationsänderungen an Firewalls und Jump-Hosts<br>▪ Kontinuierliche SIEM-Überwachung<br>▪ Vierteljährliche Zugriffsüberprüfungen<br>▪ Jährliche Überprüfung der Anwendbarkeit von kompensierenden Kontrollen<br><br>Verantwortlicher für die Überprüfung von kompensierenden Kontrollen: Leiter der Informationssicherheit<br><br>Häufigkeit der Überprüfung: Jährlich |

# Ausgefülltes Beispiel für eine Entität: Kontrollmatrix für den kundenspezifischen Ansatz

*Beachten Sie, dass dies lediglich als Beispiel für eine Möglichkeit zur Erstellung einer Kontrollmatrix im Rahmen eines kundenspezifischen Ansatzes dient und nicht als Beispiel für eine konkrete Kontrolle gedacht ist, die für eine bestimmte Umgebung geeignet oder deren Einsatz dort empfohlen wird.*

| **Kontrollmatrix Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel**<br>**Von der zu bewertenden Entität auszufüllen** | | |
|---|---|---|
| Kundenspezifischer Kontrollname/Kennung | Stimmidentifizierung und -authentifizierung | |
| PCI DSS-Anforderungsnummer und Ziel(e), die durch diese Kontrolle(n) erfüllt werden | Anforderung #: 8.2.8 | Ziel: Eine Benutzersitzung darf nur von dem autorisierten Benutzer genutzt werden. |
| **Details der Kontrolle(n)** | | |
| **Was** ist die implementierte Kontrolle(n) | Die Entität betreibt aus Gründen der Betriebshygiene eine „Zero-Touch“-Umgebung. Anstatt sich über eine Tastatur anzumelden, geben die Benutzer in einer bestimmten Umgebung ihrem Computer ausschließlich verbale Befehle.<br>Beim erstmaligen Anmelden an einem System gibt der Benutzer den Stimmbefehl „Benutzernamen erkennen“, z. B. „Alice erkennen“.<br>Das System identifiziert und authentifiziert den Benutzer zunächst über seinen einzigartigen Stimmabdruck und anschließend über einen Anruf beim physischen Zugriffskontrollsystem, welches bestätigt, dass der Benutzer sich physisch in der Umgebung befindet. Es wird dann den Benutzer (z. B. Alice) fragen, drei zufällig auf dem Bildschirm angezeigte Wörter zu wiederholen, um eine Voraufzeichnung zu verhindern, und auch zweite Überprüfung des Stimmabdrucks durchzuführen. Zu diesem Zeitpunkt ist der Benutzer angemeldet.<br>Das System ist ständig auf Stimmbefehle eingestellt. Die Sitzung des angemeldeten Benutzers ist aktiv, solange sich der Benutzer im physischen Bereich aufhält; sie wird beendet, sobald der Benutzer den Bereich mit seiner Zugangskarte verlässt. | |

| Kontrollmatrix Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von der zu bewertenden Entität auszufüllen | |
|---|---|
| | Jedes Mal, wenn der Benutzer einen Befehl erteilt, wird sein Stimmabdruck überprüft. Stimmt er nicht mit der des angemeldeten Benutzers überein, wird er abgelehnt und protokolliert. Die Protokolle werden vom SIEM verarbeitet.<br>Wenn ein anderer Benutzer versucht, das Terminal zu benutzen, an dem der Benutzer gerade angemeldet ist, stimmt der Stimmabdruck nicht überein, und das System lehnt den Befehl ab.<br>Wenn beispielsweise Dave (der ein autorisierter Benutzer des Systems ist, aber nicht an Alices Terminal angemeldet ist) oder Mary (eine böswillige Angreiferin) an Alices System herantritt und sagt: „Öffne die Pod-Schachttüren“, erkennt der Computer, dass der Befehl nicht von Alice gegeben wurde, und sagt: „Das kann ich leider nicht tun“, und protokolliert außerdem einen nicht autorisierten Zugriffsversuch.<br>Zusätzlich sind USB-Schnittstellen und Bluetooth auf den Systemen deaktiviert, sodass das Stimmerkennungssystem nicht manuell umgangen werden kann. |
| **Wo** ist/sind die Kontrolle(n) implementiert? | Produktionsstätte 17. Nevada. |
| **Wann** wird die(n) Kontrolle(n) durchgeführt? | Jedes Mal, wenn eine Stimmanfrage analysiert wird. |
| **Wer** hat Gesamtverantwortung und Rechenschaftspflicht für die Kontrolle(n)? | Der Leiter der Informationssicherheit |
| **Wer** ist er an der Verwaltung, Aufrechterhaltung und Überwachung der Kontrolle(n) beteiligt? | Die Abteilung für die Registrierung im sicheren Betriebsablauf ist für die Einarbeitung neuer Systembenutzer zuständig, was die Schulung der Benutzer und die Beschaffung von ausreichend Stimmproben umfasst, um einen zuverlässigen Stimmabdruck zu erstellen.<br>Die Verwaltung und Aufrechterhaltung des Systems wird an Acme Voiceprint Security Technologies ausgelagert, die gemäß Anforderung 12.8 verwaltet wird und diese Technologie auch vielen führenden Finanzinstituten zur Betrugserkennung und -validierung sowie zum Zugriff auf Kundendaten in Kontaktzentren zur Verfügung stellt. |
| ***Für jede* PCI-DSS-Anforderung, für die die Kontrolle(n) eingesetzt wird (werden), stellt die Entität Details zu folgenden Punkten bereit:** | |
| Die Entität beschreibt, inwiefern die implementierte(n) Kontrolle(n) das **Ziel** der PCI-DSS-Anforderung erfüllen. | Nur der angemeldete Benutzer kann eine Sitzung nutzen, da der Benutzer bei jeder Befehlseingabe faktisch erneut authentifiziert wird (mittels biometrischer Stimmabdruckerkennung). Andere autorisierte und nicht autorisierte Benutzer können die angemeldete Sitzung nicht nutzen. |

| Kontrollmatrix Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von der zu bewertenden Entität auszufüllen | |
|---|---|
| Die Entität beschreibt die von ihr **durchgeführten** Test und deren Ergebnisse, aus denen hervorgeht, dass die Kontrolle(n) das Ziel der geltenden Anforderung erfüllen. | Eine Sicherheitsbewertung wurde bei Acme Secure Testing Services in Auftrag gegeben, um die Funktionsfähigkeit des Systems zu überprüfen und einen unbefugten Zugriff auf eine Benutzersitzung zu erlangen. Das gelang ihnen nicht.<br>Unabhängig davon führte dasselbe Unternehmen eine Red-Team-Übung durch und war auch nicht in der Lage, das System zu kompromittieren und sich nicht autorisieren Zugriff zu verschaffen, indem es sich als autorisierter Stimmbenutzer ausgab. |
| Die Entität beschreibt kurz die Ergebnisse der von ihr **durchgeführten** separaten Risikoanalyse, in der die implementierten Kontrollen erläutert werden und sie beschreibt, inwiefern die Ergebnisse verifizieren, dass diese Kontrolle(n) ein Schutzniveau gewährleisten, das mindestens dem des definierten Ansatzes für die jeweilige PCI DSS-Anforderung entspricht. Einzelheiten zur Dokumentation dieser Risikoanalyse finden Sie in der separaten Vorlage für die gezielte Risikoanalyse. | Bei der definierten Anforderungskontrolle könnte ein angemeldeter Benutzer seinen Arbeitsplatz verlassen, und ein nicht autorisierter Angreifer hätte 15 Minuten Zeit, auf den Arbeitsplatz zuzugreifen, bevor die Sitzung abläuft. Mit dieser Kontrolle ist die Sitzung immer aktiv, wenn sich der Benutzer physisch in der Umgebung befindet, und der Stimmabdruck jedes Befehls wird überprüft, um sicherzustellen, dass er vom angemeldeten Benutzer stammt, bevor er ausgeführt wird.<br>Das System deckt daher ein höheres Risiko ab als die definierte Validierungskontrolle. |
| Die Entität beschreibt die Maßnahmen, die sie ergriffen hat, um sicherzustellen, dass die Kontrollmechanismen aufrechterhalten werden und ihre Wirksamkeit kontinuierlich gewährleistet ist. *Beispielsweise, wie die Entität die Wirksamkeit der Kontrollmechanismen überwacht, wie Kontrollversagen erkannt und darauf reagiert wird und welche Maßnahmen ergriffen werden.* | Jeden Monat wird ein Mitglied des GRC-Teams versuchen, eine Benutzersitzung zu übernehmen, indem es in der Einrichtung Stimmbefehle erteilt und zuvor aufgezeichnete Stimmen verwendet. Diese Übung erfolgt nach einem dokumentierten Ablauf, und die Ergebnisse werden vom System als Audioaufzeichnung gespeichert. Die Audioaufzeichnungen und die Verfahrensprotokolle werden nach jedem Test vom Leiter des Bereichs Governance, Risk und Compliance überprüft.<br>Es gibt ein Verfahren zur Meldung verdächtiger Ereignisse. Wenn ein Benutzer den Verdacht hat, dass das System auf eine nicht angemeldete Stimme reagiert hat, muss er ein bestimmtes Verfahren befolgen. Alle Benutzer wurden in der Anwendung dieses Verfahrens geschult und haben einen Scheinereignisbericht ausgefüllt. Die Verwendung dieses Verfahrens ist Bestandteil der jährlichen Sicherheitsschulung der Benutzer. Bislang wurden keine Ereignisse gemeldet. |

# Ausgefülltes Beispiel für eine Entität: Gezielte Risikoanalyse für den kundenspezifischen Ansatz

*Beachten Sie, dass dies lediglich als Beispiel für eine Möglichkeit zur Durchführung einer gezielten Risikoanalyse im Rahmen eines kundenspezifischen Ansatzes dient und nicht als Beispiel für eine konkrete Kontrolle gedacht ist, die für eine bestimmte Umgebung geeignet oder deren Einsatz dort empfohlen wird.*

| Gezielte Risikoanalyse für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von der zu bewertenden Entität auszufüllen | |
|---|---|
| **Punkt** | **Details** |
| **1. Identifizieren Sie die Anforderung** | |
| **1.1** Identifizieren Sie die PCI-DSS-Anforderung in ihrer schriftlichen Form. | 8.2.8 Wenn eine Benutzersitzung länger als 15 Minuten inaktiv war, muss sich der Benutzer erneut authentifizieren, um das Terminal oder die Sitzung wieder zu aktivieren. |
| **1.2** Identifizieren Sie das Ziel der PCI-DSS-Anforderung in ihrer schriftlichen Form. | Eine Benutzersitzung darf nur von dem autorisierten Benutzer genutzt werden. |
| **1.3** Beschreiben Sie den Missbrauch, den diese Anforderung verhindern soll. | Ein interner oder externer Angreifer kann die unbeaufsichtigte Sitzung eines legitimen Benutzers übernehmen. Der Angreifer wäre in der Lage, Aktionen durchzuführen, auf Daten zuzugreifen und Befehle zu erteilen, die fälschlicherweise dem angemeldeten Benutzer zugeschrieben würden.<br>Es könnte zu nicht autorisiertem Zugriff auf Systeme und Daten kommen.<br>Die Protokolldateien wären ungenau, da sie die Identität des angemeldeten Benutzers für Aktivitäten aufzeichnen würden, die dieser gar nicht durchgeführt hat. |
| **2. Beschreiben Sie die vorgeschlagene Lösung** | |
| **2.1** Kundenspezifischer Kontrollname/Kennung | Stimmidentifizierung und -authentifizierung |
| **2.2** Welche Teile der Anforderung, wie sie derzeit formuliert ist, werden sich in der vorgeschlagenen Lösung ändern? | Das derzeit verwendete System unterscheidet nicht ausdrücklich zwischen aktiven und inaktiven Zuständen und ist daher nicht in der Lage zu erkennen, dass eine Sitzung seit 15 Minuten „inaktiv“ ist. Stattdessen kann ein angemeldeter Benutzer dem System jederzeit nach der ersten Authentifizierung und Anmeldung einen Stimmbefehl erteilen; jeder erteilte Befehl wird jedoch überprüft, um sicherzustellen, dass er tatsächlich von dem angemeldeten Benutzer stammt.<br>Es werden nur Befehle akzeptiert, die vom angemeldeten Benutzer eingegeben werden. |
| **2.3** Wie wird die vorgeschlagene Lösung den Missbrauch verhindern? | Da jeder Stimmbefehl vor der Ausführung überprüft wird, scheitern alle Befehle, die von einer anderen Person als dem angemeldeten Benutzer erteilt werden, bei der Überprüfung und werden vom System nicht ausgeführt. Dies verhindert somit, dass ein interner oder externer Angreifer die unbeaufsichtigte Sitzung eines legitimen Benutzers übernehmen kann. |

| Gezielte Risikoanalyse für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von der zu bewertenden Entität auszufüllen | | | | | | |
|---|---|---|---|---|---|---|
| **Punkt** | **Details** | | | | | |
| **3. Analysieren Sie etwaige Veränderungen hinsichtlich der WAHRSCHEINLICHKEIT, dass der Missbrauch eintritt, der zu einer Verletzung der Vertraulichkeit von Karteninhaberdaten führt** | | | | | | |
| **3.1** Beschreiben Sie die in der Kontrollmatrix aufgeführten Faktoren, die die Wahrscheinlichkeit des Eintritts des Missbrauchs beeinflussen. | Jeder vom System empfangene Befehl wird darauf validiert, ob er tatsächlich vom angemeldeten Benutzer erteilt wurde. Dies verringert die Wahrscheinlichkeit, dass eine angemeldete Sitzung von einem Angreifer übernommen wird. Unter der definierten Anforderung hat ein Angreifer ein Zeitfenster von 15 Minuten, um physischen Zugriff auf eine unbeaufsichtigte, authentifizierte Sitzung zu erlangen und diese zu übernehmen.<br>Bei den eingesetzten Kontrollen besteht für einen Angreifer keine Möglichkeit, Befehle unter der Sitzung eines angemeldeten Benutzers auszuführen. | | | | | |
| **3.2** Beschreiben Sie die Gründe, warum der Missbrauch auch nach der Anwendung der kundenspezifischen Kontrolle weiterhin auftreten kann. | Das System wurde ausgiebig getestet und lässt sich nicht durch technische Lösungen wie Stimmsynthese und die Wiedergabe von Aufnahmen überlisten; es ist davon auszugehen, dass selbst entsprechende Versuche vom angemeldeten Benutzer bemerkt würden, der sich physisch in der Umgebung aufhalten muss, um angemeldet zu bleiben.<br>Ein Angreifer könnte diese Kontrolle durch physische Einschüchterung des angemeldeten Benutzers umgehen; das System ist jedoch mit einem Notfallmonitor ausgestattet, der dem Benutzer keine Hinweise auf eine Aktivierung gibt, aber das Sicherheitspersonal alarmiert.<br>Bei Sicherheitstests und Evaluierungsverfahren konnte das System von einem simulierten Angreifer nicht umgangen werden. | | | | | |
| **3.3** Inwieweit stellen die im kundenspezifischen Ansatz beschriebenen Kontrollen im Vergleich zu den Anforderungen des definierten Ansatzes eine Veränderung der Wahrscheinlichkeit dar, dass der Missbrauch auftritt? | Es ist wahrscheinlicher, dass Missbrauch auftritt | ☐ | Keine Änderung | ☐ | Es ist weniger wahrscheinlich, dass Missbrauch auftritt | ☒ |
| **3.4** Stellen Sie die Begründung Ihrer Bewertung hinsichtlich der Veränderung der Wahrscheinlichkeit, dass der Missbrauch auftritt, bereit sobald die kundenspezifischen Kontrollen eingeführt sind. | Das 15-minütige Zeitfenster, das einem Angreifer gemäß der Anforderung zur Übernahme der Sitzung eines angemeldeten Benutzers zur Verfügung steht, wird auf null Minuten reduziert, da bei jedem Befehl überprüft wird, ob er tatsächlich vom angemeldeten Benutzer stammt. | | | | | |

| Gezielte Risikoanalyse für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von der zu bewertenden Entität auszufüllen | | | | |
|---|---|---|---|---|
| **Punkt** | **Details** | | | |
| **4. Analysieren Sie alle Veränderungen der AUSWIRKUNGEN eines nicht autorisierten Zugriffs auf Kontodaten** | | | | |
| **4.1** Angesichts des Umfangs der Systemkomponenten, die diese Lösung abdeckt: Welches Volumen an Kontodaten wäre im Falle eines Ausfalls der Lösung dem Risiko eines nicht autorisierten Zugriffs ausgesetzt? | **4.1.1** Anzahl der gespeicherten PANs | Keine. Die Entität speichert keine PAN. | **4.1.2** Anzahl der PANs, die innerhalb eines Zeitraums von 12 Monaten verarbeitet oder übertragen wurden | 32 Millionen |
| **4.2** Beschreibung, wie die kundenspezifischen Kontrollen direkt:<br>Die Anzahl der betroffenen individuellen PANs verringern, falls ein Angreifer erfolgreich ist, und/oder<br>Eine schnellere Benachrichtigung der Kreditkartenunternehmen über kompromittierte PANs ermöglichen. | Die eingesetzten Kontrollen stellen keine Verringerung der Auswirkungen eines nicht autorisierten Zugriffs auf Kontodaten bereit. | | | |
| **5. Risikogenehmigung und -prüfung** | | | | |
| **5.1** Ich habe die obige Risikoanalyse geprüft und stimme zu, dass die Verwendung des vorgeschlagenen, individuell angepassten Ansatzes, wie detailliert beschrieben, mindestens ein gleichwertiges Schutzniveau bietet wie der definierte Ansatz für die jeweilige PCI DSS-Anforderung. | [Unterschrift] | | | |
| **5.2** Diese Risikoanalyse muss spätestens bis zum folgenden Zeitpunkt überprüft und aktualisiert werden: | [Datum] | | | |

# Ausgefülltes Beispiel für den Bewerter: Konformitätsbericht – Anhang E: Vorlage für einen kundenspezifischen Ansatz

*Beachten Sie, dass dies lediglich als Beispiel für eine Möglichkeit zur Erstellung des Konformitätsberichts dient und nicht als Beispiel für eine konkrete Kontrollmaßnahme gedacht ist, die für eine bestimmte Umgebung geeignet oder deren Einsatz dort empfohlen wird.*

**Anforderungsnummer und Definition:** PCI DSS-Anforderung 8.2.8: Wenn eine Benutzersitzung länger als 15 Minuten inaktiv war, muss sich der Benutzer erneut authentifizieren, um das Terminal oder die Sitzung wieder zu aktivieren.

| Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von dem Bewerter auszufüllen | |
|---|---|
| **Identifizieren Sie den kundenspezifischen Kontrollnamen/Kennung** jeder einzelnen Kontrolle, die zur Erreichung des Ziels des kundenspezifischen Ansatzes verwendet wird.<br>*(**Hinweis**: Verwenden Sie den Namen der kundenspezifischen Kontrolle aus der Kontrollmatrix der bewerteten Entität.)* | Stimmidentifizierung und -authentifizierung |
| **Beschreiben Sie jede einzelne Kontrolle**, die zur Erreichung des Ziels des kundenspezifischen Ansatzes verwendet wird.<br>***(Hinweis:** Siehe die Anforderungen und Testverfahren des Payment Card Industry Data Security Standard (PCI DSS) für das Ziel kundenspezifischer Ansatz.* | Ziel: Eine Benutzersitzung darf nur von dem autorisierten Benutzer genutzt werden.<br>1. Die Benutzer melden sich ausschließlich über Stimmbefehle im System an. Das System identifiziert und authentifiziert den Benutzer zunächst über seinen einzigartigen Stimmabdruck und anschließend über einen Anruf beim physischen Zugriffskontrollsystem, welches bestätigt, dass der Benutzer sich physisch in der Umgebung befindet. Das System fragt dann den Benutzer, drei zufällig auf dem Bildschirm angezeigte Wörter zu wiederholen, um eine Voraufzeichnung zu verhindern, und führt eine zweite Überprüfung des Stimmabdrucks durch.<br>2. Das System ist ständig auf Stimmbefehle eingestellt. Die Sitzung des angemeldeten Benutzers ist aktiv, solange sich der Benutzer im physischen Bereich aufhält; sie wird beendet, sobald der Benutzer den Bereich mit seiner Zugangskarte verlässt.<br>3. Jedes Mal, wenn der Benutzer einen Befehl erteilt, wird sein Stimmabdruck überprüft. Stimmt er nicht mit der des angemeldeten Benutzers überein, wird er abgelehnt und protokolliert. Die Protokolle werden vom SIEM verarbeitet. |

| Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von dem Bewerter auszufüllen | |
|---|---|
| | 4. Wenn ein anderer Benutzer versucht, das Terminal zu benutzen, an dem der Benutzer gerade angemeldet ist, stimmt der Stimmabdruck nicht überein, und das System lehnt den Befehl ab.<br>5. USB-Schnittstellen und Bluetooth sind auf den Systemen deaktiviert, sodass das Stimmerkennungssystem nicht manuell umgangen werden kann. |
| **Beschreiben Sie, inwiefern** die Kontrolle(n) das Ziel des kundenspezifischen Ansatzes erfüllen. | Kundenspezifisches Ansatzziel: Eine Benutzersitzung darf nur von dem autorisierten Benutzer genutzt werden.<br>Nur der angemeldete Benutzer kann eine Sitzung nutzen, da der Benutzer bei jeder Befehlseingabe faktisch erneut authentifiziert wird (mittels biometrischer Stimmabdruckerkennung). Andere autorisierte und nicht autorisierte Benutzer können die angemeldete Sitzung nicht nutzen. |
| **Identifizieren Sie die geprüfte Dokumentation zur Kontrollmatrix**, die einen kundenspezifischen Ansatz für diese Anforderung stützt. | Dok-10 – Kundenspezifischer Ansatz-Kontrollmatrix |
| **Identifizieren Sie die geprüfte Dokumentation zur gezielten Risikoanalyse**, die den kundenspezifischen Ansatz für diese Anforderung unterstützt. | Dok-11 – Kundenspezifischer Ansatz TRA |
| **Identifizieren Sie den/die Namen des/der Bewerter(s) an, der/die bestätigt, dass:**<br>Die Entität hat die Kontrollmatrix unter Einbeziehung aller in der Vorlage für die Kontrollmatrix in PCI DSS v4.x angegebenen Informationen abgeschlossen: Beispielvorlagen zur Unterstützung des kundenspezifischen Ansatzes auf der PCI SSC-Webseite, und die Ergebnisse der Kontrollmatrix unterstützen den kundenspezifischen Ansatz für diese Anforderung.<br>Die Entität hat die gezielte Risikoanalyse abgeschlossen, einschließlich aller in der Vorlage für die gezielte Risikoanalyse in PCI DSS v4.x angegebenen Informationen: Beispielvorlagen zur Unterstützung des kundenspezifischen Ansatzes auf der PCI SSC-Webseite und dass die Ergebnisse der Risikoanalyse die Verwendung des kundenspezifischen Ansatzes für diese Anforderung unterstützen. | Josephine Bewerter |

| Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von dem Bewerter auszufüllen | | |
|---|---|---|
| **Beschreiben Sie** die vom Bewerter abgeleiteten und durchgeführten **Testverfahren**, um **zu validieren, dass die implementierten Kontrollen das Ziel des kundenspezifischen Ansatzes erfüllen**; beispielsweise, ob die kundenspezifische(n) Kontrolle(n) ausreichend robust ist/sind, um mindestens ein gleichwertiges Schutzniveau wie vom definierte Ansatz bereitgestellt zu gewährleisten.<br>***Hinweis 1:*** *Technische Überprüfungen (z. B. Überprüfung der Konfigurationseinstellungen, der Betriebseffizienz usw.) sollten, soweit möglich und angemessen, durchgeführt werden.*<br>***Hinweis 2:*** *Fügen Sie bei Bedarf für jedes vom Bewerter festgelegte Testverfahren weitere Zeilen hinzu. Stellen Sie sicher, dass bei jedem hinzugefügten, vom Bewerter festgelegten Testverfahren alle Zeilen rechts neben dem Eintrag „Vom Bewerter abgeleitetes Testverfahren" kopiert werden.* | | |
| Geben Sie hier das vom Bewerter festgelegte Testverfahren ein:<br>1.a) Versuchen Sie, nachdem Sie Zugriff auf die Umgebung erhalten haben, sich über die vorhandene Tastatur – sofern vorhanden – beim System anzumelden.<br>1.b) Versuchen Sie, nachdem Sie Zugriff auf die Umgebung erhalten haben, sich über den erforderlichen Stimmbefehl beim System anzumelden. | **Identifizieren Sie, was getestet wurde** (zum Beispiel befragte Personen, überprüfte Systemkomponenten, beobachtete Prozesse usw.)<br>***Hinweis:*** *Alle getesteten Punkte müssen eindeutig identifiziert werden.* | Es wurden Tests mit Hilfe von Int-1, Int-2 und Int-3 in der Produktionsanlage 17 in Nevada auf KonsoleA und KonsoleB durchgeführt, wo die kundenspezifische Ansatzkontrolleaktiv ist.<br>Es wurde mit Int-10 gesprochen, um zu verifizieren, ob die bei den Tests 1 und 2 aufgetretenen Anomalien erfasst und überprüft wurden. |
| | **Identifizieren Sie alle** im Rahmen dieses Testverfahrens untersuchten **Nachweise**. | Dok-22 wurde geprüft – SIEM-Protokoll für den Zeitraum der Tests 1 und 2. |

## Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel

### Von dem Bewerter auszufüllen

| | | |
|---|---|---|
| 1.c) Nachdem sich der autorisierte Benutzer im System angemeldet hat, wiederholen Sie die drei zufällig ausgewählten Wörter, die auf dem Bildschirm angezeigt werden.<br><br>1.d) Nachdem sich der Benutzer am System angemeldet hat, soll ein anderer autorisierter Benutzer die drei auf dem Bildschirm angezeigten Zufallswörter wiederholen.<br><br>2.a) Geben Sie, während sich der autorisierte Benutzer im Raum befindet, einen Stimmbefehl mit der Stimme des Bewerters.<br><br>2.b) Nachdem der autorisierte Benutzer den Bereich mit seiner Zugangskarte verlassen hat, geben Sie einen Stimmbefehl an das System, wobei Sie eine Stimmaufzeichnung verwenden, in der der Benutzer den Befehl erteilt.<br><br>3.a) Überprüfen Sie die SIEM-Protokolle auf die Ergebnisse der Tests 1 und 2.<br><br>3.b) Sprechen Sie mit den Mitarbeitern, die für die Überprüfung des SIEM-Protokolls zuständig sind, um zu bestimmen, ob sie bei den Tests 1 und 2 irgendwelche Anomalien erfasst haben.<br><br>4.a) In 2.b. getestet.<br><br>5.a) Untersuchen Sie das System auf USB-Schnittstellen und Bluetooth-Funktionen. | **Beschreiben Sie die Ergebnisse** der vom Bewerter im Rahmen dieses Testverfahrens durchgeführten Tests und wie diese Ergebnisse verifizieren, dass die implementierten Kontrollen das kundenspezifische Ansatzziel erfüllen. | Der Bewerter folgte einem autorisierten Benutzer in die Umgebungen, in denen sich KonsoleA und KonsoleB befanden.<br><br>Test 5.a) Zunächst überprüfte der Bewerter die Konsolen, um sicherzustellen, dass die USB-Schnittstellen und die Bluetooth-Funktionen des Systems nicht verfügbar waren.<br><br>Test 1.a) Dann beobachtete der Bewerter, dass für die Anmeldung an beiden Konsolen keine Tastaturen zur Verfügung standen.<br><br>Test 1.b) Der Bewerter versuchte dann, sich über den erforderlichen Stimmbefehl im System anzumelden. Das System gab eine Fehlermeldung aus, wonach der Bewerter kein autorisierter Benutzer sei und sich daher nicht anmelden könne.<br><br>Test 1.c) Anschließend beobachtete der Bewerter, wie sich Int-1 an jeder Konsole anmeldete, und notierte dabei die Verwendung eines Stimmbefehls, der von jeder Konsole akzeptiert wurde. Der Bewerter wiederholte dann die drei auf dem Bildschirm jeder Konsole angezeigten Wörter und stellte fest, dass das System den Benutzer nicht anmeldete und eine Fehlermeldung anzeigte, wonach die Stimmantwort des Benutzers nicht erkannt wurde.<br><br>Test 1.d) Der Bewerter beobachtete, wie Int-2 die drei zufällig auf dem Bildschirm angezeigten Wörter wiederholte. Das System verweigerte Int-2 den Zugriff und gab eine Meldung aus, dass der Stimmabdruck nicht übereinstimme.<br><br>Test 2.a) Nachdem sich Int-1 ordnungsgemäß im System angemeldet hatte und das System offenbar auf die Befehle von Int-1 zum Öffnen der Datei xyz reagierte, gab der Bewerter einen Befehl an das System, die Datei xyz zu öffnen. Das System weigerte sich, die Datei zu öffnen, und gab eine Warnmeldung aus, dass der Stimmabdruck nicht übereinstimme.<br><br>Test 2.b und Test 4.a): Der Bewerter beobachtete, wie der angemeldete Benutzer die Umgebung mit seiner Zugangskarte verließ. Nachdem der angemeldete Benutzer die Umgebung verlassen hatte, versuchte der Bewerter, einen Befehl an das System zu senden, wobei er eine Aufzeichnung nutzte, in der der vorherige Benutzer einen Befehl an das System gesendet hatte. Das System hat die Ausführung des Befehls verweigert und eine Meldung ausgegeben, dass der Benutzer vom System abgemeldet wurde. |

| Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von dem Bewerter auszufüllen | | |
|---|---|---|
| | | Test 3.a.) Der Bewerter erhielt die während der Tests erzeugten SIEM-Protokolle und stellte fest, dass das System die fehlgeschlagenen Zugriffs- und Befehlsversuche ordnungsgemäß protokolliert hatte.<br>Test 3.b) Der Bewerter befragte Int-10, um zu verifizieren, ob sie eine Benachrichtigung über den versuchten Zugriff auf das System erhalten hatte.<br>Der Bewerter stellte fest, dass die Kontrolle in ihrer vorgesehenen Form wie beabsichtigt funktioniert und dass die Konzeption offenbar wirksam dazu beiträgt, eine Benutzersitzung ausschließlich auf den Benutzer zu beschränken, der autorisierten Zugriff erhalten hat. |
| **Dokumentieren Sie** die vom Bewerter abgeleiteten und durchgeführten **Testverfahren**, um zu **validieren, dass die Kontrollen aufrechterhalten werden, um ihre fortdauernde Wirksamkeit sicherzustellen**; zum Beispiel wie die Entität die Wirksamkeit der Kontrollen überwacht und wie Kontrollversagen erkannt, darauf reagiert und welche Maßnahmen ergriffen werden.<br>***Hinweis 1:*** *Technische Überprüfungen (z. B. Überprüfung der Konfigurationseinstellungen, der Betriebseffizienz usw.) sollten, soweit möglich und angemessen, durchgeführt werden.*<br>***Hinweis 2:*** *Fügen Sie bei Bedarf für jedes vom Bewerter festgelegte Testverfahren weitere Zeilen hinzu. Stellen Sie sicher, dass bei jedem hinzugefügten, vom Bewerter festgelegten Testverfahren alle Zeilen rechts neben dem Eintrag „Vom Bewerter abgeleitetes Testverfahren" kopiert werden.* | | |
| Geben Sie hier das vom Bewerter festgelegte Testverfahren ein:<br>1) Überprüfen Sie das im GRC dokumentierte Verfahren zum monatlichen Testen der Kontrollen.<br>2) Überprüfen Sie das Datum und die Uhrzeit der Ergebnisse der letzten 12 Monate, um sicherzustellen, dass die Tests monatlich durchgeführt werden.<br>3) Wählen Sie zwei protokollierte Testergebnisse aus, um zu<br>überprüfen, ob die Kontrollen wie erwartet funktionierten und ob der Leiter der GRC die Ergebnisse geprüft hat. | **Identifizieren Sie, was getestet wurde** (zum Beispiel befragte Personen, überprüfte Systemkomponenten, beobachtete Prozesse usw.)<br>***Hinweis:*** *Alle getesteten Punkte müssen eindeutig identifiziert werden.* | GRC-Verfahren (Dok. 3) und Testergebnisse der letzten 12 Monate (Dok. 4),<br>Führte ein Gespräch mit Int-1 und überprüfte die Testergebnisse für März 2025 und August 2025 (Doc-16, Doc-17)<br>Das dokumentierte Verfahren zum Ereignisbericht wurde gemeinsam mit Int-1 überprüft.<br>Die jährlichen Sicherheitsschulungsmaterialien wurden mit den Gruppen Int-1, Int-2 und Int-3 überprüft. Die von Int-10 bis Int-14 ausgefüllten Scheinereignisberichte wurden geprüft.<br>Es wurde überprüft, dass in den letzten 12 Monaten kein Ereignis aufgetreten ist. |

| Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von dem Bewerter auszufüllen | | |
|---|---|---|
| 4) Überprüfen Sie das dokumentierte Verfahren zur Meldung verdächtiger Vorfälle und verifizieren Sie, dass darin ausreichend beschrieben ist, wie sich das Personal verhalten soll, falls das System auf eine Stimme reagiert, die nicht angemeldet ist.<br><br>5) Überprüfen Sie jährliche Sicherheitsschulungsmaterialien, um sicherzustellen, dass alle Benutzer in der Verwendung des Verfahrens geschult wurden.<br><br>6) Wählen Sie fünf zufällig ausgewählte Scheinereignisberichte aus und prüfen Sie diese auf Vollständigkeit.<br><br>7) Wenn ein verifiziertes Ereignis aufgetreten ist, überprüfen Sie den Ereignisbericht. Überprüfen Sie alle verifizierten Ereignisberichte. | **Identifizieren Sie** alle im Rahmen dieses Testverfahrens untersuchten **Nachweise.** | Test 1: Dok-3<br>Test 2: Dok-4<br>Test 3: Dok-16, Dok-17, Int-01<br>Test 4: Dok-20<br>Test 5: Dok-23<br>Test 6: Dok-50, 51, 52, 53, 54 |

| Konformitätsbericht Vorlage für den kundenspezifischen Ansatz – Ausgefülltes Beispiel<br>Von dem Bewerter auszufüllen | | |
|---|---|---|
| | **Beschreiben Sie die Ergebnisse** der vom Bewerter im Rahmen dieses Testverfahrens durchgeführten Tests und wie diese Ergebnisse verifizieren, dass die implementierten Kontrollen aufrechterhalten werden, um ihre fortwährende Wirksamkeit sicherzustellen. | Die GRC-Verfahren zum monatlichen Testen der Kontrollen scheinen klar und wirksam zu sein, um festzustellen, ob die Stimmbefehlskontrollen wie vorgesehen funktioniert. Die GRC führte die Tests monatlich durch, wobei die Ergebnisse gemäß den in den Verfahren beschriebenen Vorgaben protokolliert wurden. Die Ergebnisse schienen ausreichend dokumentiert zu sein, einschließlich des Zeitpunkts der Durchführung, der Person, die den Test durchgeführt hat, und der Testergebnisse.<br><br>Die Verfahren zur Meldung verdächtiger Ereignisse scheinen klar und angemessen zu sein. Die Berichtsanforderungen umfassen ein Formular (Ereignisbericht), das vom IT-Personal in der Produktionsstätte 17 verwendet werden muss. Nevada. Es wurde bestätigt, dass alle IT-Mitarbeiter an der Produktionsstätte 17 sind. Nevada wurde anhand des von der Personalabteilung bereitgestellten Schulungsprotokolls geschult. Außerdem wurden fünf zufällig ausgewählte Scheinereignisberichte aus den Personalakten überprüft, und es stellte sich heraus, dass diese gemäß den Vorschriften ausgefüllt worden waren.<br><br>Gemeinsam mit Int-1 wurde das von Int-1 bereitgestellte Ereignisprotokoll der letzten 12 Monate geprüft. Obwohl im Protokoll Ereignisse vermerkt waren, schien keiner davon mit der Stimmbefehlskontrolle in Zusammenhang zu stehen. Es wurde mit Int-1 bestätigt, dass es keine Ereignisse im Zusammenhang mit der Kontrolle gegeben hat.<br><br>Daher scheint die Aufrechterhaltung dieser Kontrolle die fortwährende Wirksamkeit der Beschränkung einer Benutzersitzung auf den autorisierten Benutzer zu gewährleisten, der sich am System angemeldet hat. |