Payment Card Industry (PCI)

Datensicherheitsstandard

Selbstbewertungsfragebogen C-VT

und Konformitätsbescheinigung

Händler mit webbasierten virtuellen Zahlungsterminals - ohne elektronischen Karteninhaberdaten-Speicher

Zur Verwendung in PCI-DSS, Version 3.2.1

Revision 1.0

Juni 2018

Dokumentänderungen

Datum	Version	SBF Revision	Beschreibung
Oktober 2008	1.2		Anpassung der Inhalte an den neuen PCI DSS v1.2 und Implementieren kleinerer Änderungen nach der Ursprungsversion v1.1.
Oktober 2010	2.0		Anpassung der Inhalte an die neuen Anforderungen und Testverfahren nach PCI DSS v2.0.
Februar 2014	3.0		Anpassung der Inhalte an die Anforderungen und Testverfahren nach PCI DSS v3.0 sowie Integration weiterer Reaktionsmöglichkeiten.
April 2015	3.1		Aktualisierung zur Anpassung an PCI-DSS v3.1. Weitere Informationen zu PCI-DSS-Änderungen finden Sie unter Überblick über Änderungen von PCI-DSS, Version 3.0 bis 3.1.
April 2016	3.2	1.0	Aktualisierung zur Anpassung an PCI-DSS v3.2. Weitere Informationen zu PCI-DSS-Änderungen finden Sie unter Überblick über Änderungen von PCI-DSS, Version 3.1 bis 3.2. Anforderung aus PCI DSS v3.2 hinzugefügt Anforderungen 8, 9 und Appendix A2.
Januar 2017	3.2	1.1	Änderungen am Dokument zur Klärung von Anforderungen des Updates von April 2016 aktualisiert. Fußnote zum Abschnitt zur Klärung des Zwecks der zugelassenen Systeme hinzugefügt. Anforderung 8.3.1 zur Anpassung von Anforderung 2.3 hinzugefügt. Anforderung 11.3.4 zur Überprüfung von Segmentierungskontrollen hinzugefügt, wenn Segmentierung verwendet wird.
Juni 2018	3.2.1	1.0	Aktualisierung zur Anpassung an PCI-DSS v3.2.1. Weitere Informationen zu PCI-DSS-Änderungen finden Sie unter Überblick über Änderungen von PCI-DSS, Version 3.2 bis 3.2.1.

Inhalt

Vorbereitung

Der SBF C-VT wurde entwickelt, um die Anforderungen an Händler anzusprechen, die Karteninhaberdaten nur mithilfe eigenständiger virtueller Zahlungsterminals auf einem PC mit Internetanschluss verarbeiten.

Ein virtuelles Zahlungsterminal ist ein Webbrowser-basierter Zugriffspunkt auf die Website eines Acquirers, eines Verarbeitungsunternehmens oder eines Drittanbieters zur Autorisierung von Transaktionen mit Zahlungskarten; auf dieser Website gibt ein Händler manuell Karteninhaberdaten über einen sicher verbundenen Webbrowser ein. Anders als physische Terminals lesen virtuelle Zahlungsterminals Daten nicht direkt von Zahlungskarten. Da die Transaktionen mit Zahlungskarten manuell eingegeben werden, werden in Händlerumgebungen mit niedrigen Transaktionsvolumen virtuelle Zahlungsterminals häufig anstatt physischer Terminals eingesetzt.

SBF-C-VT-Händler verarbeiten Karteninhaberdaten nur über ein virtuelles Zahlungsterminal und speichern keine Karteninhaberdaten auf Computersystemen. Diese virtuellen Terminals sind mit dem Internet verbunden, um sich mit dem Drittanbieter in Kontakt zu setzen, der die Zahlungsabwicklungsfunktion auf dem virtuellen Terminal hostet. Dieser Drittanbieter kann entweder ein Verarbeitungsunternehmen, ein Acquirer oder ein anderer Drittdienstanbieter sein, der Karteninhaberdaten speichert, verarbeitet und/oder überträgt, um die Zahlungstransaktionen auf virtuellen Terminals von Händlern zu autorisieren und/oder abzuwickeln.

Diese SBF-Option gilt nur für Händler, die gleichzeitig immer nur eine Transaktion manuell über eine Tastatur einer internetbasierten virtuellen Terminallösung eingeben. SBF C-VT Händler können Händler mit Verkaufsräumlichkeiten (vorliegende Karte) oder Versandhändler sein.

SBF-C-VT-Händler bestätigen im Zusammenhang mit diesem Zahlungskanal folgende Bedingungen:

- Die Zahlungsvorgänge Ihres Unternehmens werden über ein virtuelles Zahlungsterminal abgewickelt, auf das über einen mit dem Internet verbundenen Webbrowser zugegriffen wird.
- Die virtuelle Zahlungsterminallösung des Unternehmens wird von einem PCI DSS-validierten Drittanbieter bereitgestellt und gehostet.
- Ihr Unternehmen greift auf die PCI-DSS-konforme virtuelle Zahlungsterminal-Lösung über einen isolierten Computer einer einzelnen Stelle zu, der innerhalb Ihrer Umgebung weder mit anderen Stellen noch Systemen verbunden ist (diese Eigenschaft kann mithilfe einer Firewall- oder Netzwerksegmentierung erreicht werden, um den Computer von anderen Systemen zu trennen).
- Auf dem Computer des Unternehmens ist keine Software installiert, die die Speicherung von Karteninhaberdaten bewirkt (beispielsweise Software für Stapelverarbeitung oder Teilstreckenverfahren).
- Am Computer des Unternehmens sind keine Hardwaregeräte zur Erfassung oder Speicherung von Karteninhaberdaten angeschlossen (beispielsweise Kartenleser).
- Ihr Unternehmen empfängt oder überträgt auch anderweitig über andere Kanäle keine Karteninhaberdaten (z. B. über ein internes Netzwerk oder das Internet).
- Alle von Ihrem Unternehmen aufbewahrten Daten des Karteninhabers liegen auf Papier vor (z. B. ausgedruckte Berichte oder Belege) und diese Dokumente wurden nicht elektronisch erhalten **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Dieser SBF gilt nicht für E-Commerce-Kanäle.

[1] Dieses Kriterium soll nicht mehr als ein zugelassenes System (also IP-verbundene POI-Geräte) sperren, die sich in derselben Netzwerkzone befinden, solange die zugelassenen Systeme von anderen Arten von Systemen isoliert sind (z. B. durch Implementierung von Netzwerksegmentierung). Darüber hinaus soll dieses Kriterium den definierten Systemtyp nicht an der Übermittlung von Transaktionsinformationen an Dritte zum Zwecke der Verarbeitung über ein Netzwerk hindern, wie z. B. ein Acquirer oder Zahlungsverarbeiter.

Diese gekürzte Version des SBF enthält Fragen, die sich auf eine bestimmte Kleinhändlerumgebung, wie in den oben beschriebenen Qualifikationskriterien beschrieben, beziehen. Sollten für Ihre Umgebung PCI-DSS-Anforderungen gelten, die nicht in diesem SBF behandelt werden, kann dies ein Hinweis darauf sein, dass dieser SBF nicht für Ihr Unternehmen geeignet ist. Zusätzlich müssen Sie auch weiterhin alle geltenden PCI-DSS-Anforderungen erfüllen, um als PCI-DSS-konform angesehen zu werden.

PCI-DSS-Selbstbeurteilung - Schritte zum Ausfüllen

1. Stellen Sie fest, welcher SBF für Ihre Umgebung relevant ist - Nähere Informationen finden Sie im Dokument "Anleitung und Richtlinien zum Selbstbeurteilungsfragebogen" auf der PCI SSC-Website.
2. Bestätigen Sie, dass Ihre Umgebung dem Umfang/Geltungsbereich entspricht und die Qualifikationskriterien für den von Ihnen verwendeten SBF erfüllt (gemäß Definition in Teil 2g der Konformitätsbescheinigung).
3. Beurteilen Sie Ihre Umgebung hinsichtlich der Konformität mit den entsprechenden PCI-DSS-Anforderungen.
4. Füllen Sie alle Abschnitte des Dokuments aus:
   - Abschnitt (Teil 1 und 2 der Konformitätsbescheinigung) - Informationen zur Beurteilung und Executive Summary.
   - Abschnitt - PCI-DSS-Selbstbeurteilungsfragebogen (SBF C-VT)
   - Abschnitt (Teil 3 und 4 der Konformitätsbescheinigung) - Validierungs- und Bescheinigungsdetails sowie Aktionsplan für nicht konforme Anforderungen (falls zutreffend)
5. Reichen Sie den SBF und die Konformitätsbescheinigung (AOC) zusammen mit allen anderen erforderlichen Dokumenten - zum Beispiel den ASV-Scan-Berichten - beim Acquirer, bei der Zahlungsmarke oder bei einer anderen Anforderungsstelle ein.

Erklärungen zum Selbstbeurteilungsfragebogen

Die Fragen in der Spalte "PCI-DSS-Frage" in diesem Selbstbeurteilungsfragebogen basieren auf den PCI-DSS-Anforderungen.

Als Hilfe beim Beurteilungsprozess stehen weitere Ressourcen mit Hinweisen zu den PCI-DSS- Anforderungen und zum Ausfüllen des Selbstbeurteilungsfragebogens zur Verfügung. Ein Teil dieser Ressourcen ist unten aufgeführt:

Dokument	Inhalt:
PCI DSS (Anforderungen und Sicherheitsbeurteilungsverfahren des PCI-Datensicherheitsstandards)	• Leitfaden zum Umfang/Geltungsbereich • Leitfaden zum Zweck der PCI-DSS-Anforderungen • Detaillierte Informationen zu Testverfahren • Leitfaden zu Kompensationskontrollen
Anleitung und Richtlinien zum SBF	• Informationen zu allen SBF und ihren Qualifikationskriterien • Bestimmung des passenden SBF für Ihr Unternehmen
PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme	• Beschreibungen und Definitionen von Begriffen, die im PCI DSS und in den Selbstbeurteilungsfragebögen vorkommen

Diese und weitere Ressourcen sind auf der PCI-SSC-Website (www.pcisecuritystandards.org) zu finden. Unternehmen sollten vor jeder Beurteilung den PCI DSS und weitere zugehörige Dokumente durchlesen.

Ausfüllen des Selbstbeurteilungsfragebogens

Für jede Frage stehen mehrere Antwortmöglichkeiten zur Auswahl, die den Status Ihres Unternehmens in Bezug auf die jeweilige Anforderung widerspiegeln. **Für jede Frage sollte nur eine Antwortmöglichkeit gewählt werden.**

In der nachstehenden Tabelle finden Sie eine Beschreibung der Bedeutung der einzelnen Antwortmöglichkeiten:

Antwort	Wann trifft diese Antwort zu?
Ja	Die erwarteten Tests wurden durchgeführt und alle Elemente der Anforderung wurden wie angegeben erfüllt.
Ja, mit CCW (Compensating Control Worksheet, Arbeitsblatt zu Kompensationskontrollen)	Die erwarteten Tests wurden durchgeführt, und die Anforderung wurde unter Zuhilfenahme einer Kompensationskontrolle erfüllt. Für alle Antworten in dieser Spalte ist ein Arbeitsblatt zu Kompensationskontrollen (Compensating Control Worksheet, CCW) in Anhang B des SBF auszufüllen. Informationen zu Kompensationskontrollen und Hinweise zum Ausfüllen des Arbeitsblatts sind im PCI DSS enthalten.
Nein	Einige oder alle Elemente der Anforderung wurden nicht erfüllt, werden gerade implementiert oder müssen weiteren Tests unterzogen werden, ehe bekannt ist, ob sie vorhanden sind.
Nicht zutr. (Nicht zutreffend)	Die Anforderung gilt nicht für die Umgebung des Unternehmens. (Beispiele finden Sie im Leitfaden zur Nichtanwendbarkeit bestimmter spezieller Anforderungen.) Bei allen Antworten in dieser Spalte ist eine zusätzliche Erklärung in Anhang C des SBF erforderlich.

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

Während viele Unternehmen, die SBF B-IP ausfüllen, die Konformität mit allen PCI-DSS-Anforderungen bestätigen müssen, werden einige Unternehmen mit sehr spezifischen Geschäftsmodellen eventuell feststellen, dass einige Anforderungen für sie nicht gelten. Ein Unternehmen, das z. B. überhaupt keine drahtlose Technologie verwendet, muss die Konformität mit den Abschnitten des PCI DSS, die sich speziell auf die Verwaltung drahtloser Technologien beziehen, nicht validieren (etwa die Anforderungen 1.2.3, 2.1.1 und 4.1.1).

Gelten einzelne Anforderungen als nicht anwendbar in Ihrer Umgebung, wählen Sie für die betreffenden Anforderungen die Option "Nicht zutr." und füllen Sie zu jedem "Nicht zutr."-Eintrag das Arbeitsblatt "Erklärung der Nichtanwendbarkeit" in Anhang C aus.

Gesetzliche Ausnahme

Unterliegt Ihr Unternehmen einer gesetzlichen Beschränkung, welche die Erfüllung einer PCI-DSS- Anforderung unmöglich macht, markieren Sie für diese Anforderung die Spalte "Nein" und füllen Sie die zugehörige Bescheinigung in Teil 3 aus.

Abschnitt 1: Informationen zur Beurteilung

Anweisungen zur Einreichung

Dieses Dokument muss zur Bestätigung der Ergebnisse der Händler-Selbstbeurteilung gemäß dem *Datensicherheitsstandard der Zahlungskartenbranche (Payment Card Industry Data Security Standard, kurz PCI-DSS) und den Sicherheitsbeurteilungsverfahren ausgefüllt werden.* Füllen Sie alle Abschnitte aus: Der Händler ist dafür verantwortlich, dass alle Abschnitte von den betreffenden Parteien ausgefüllt werden. Wenden Sie sich bezüglich des ordnungsgemäßen Berichts- und Einreichungsverfahrens an den Acquirer (Handelsbank) oder die Zahlungsmarken.

Teil 1. Informationen zum Qualified Security Assessor und Händler			
Teil 1a. Händlerinformationen			
Firmenname:	Hohmann Weinbau Rügen GmbH	DBA (Geschäftstätigkeit als):	Hohmann Weinbau Rügen GmbH
Kontaktname:	Simone Hantke	Titel:	
ISA-Name(n) (falls zutreffend):		Titel:	
Telefon:	41795998936	E-Mail:	hohmann@weingut-ruegen.com
Geschäftsadresse:	DorstraBe 16 16		
	18586		
	Lancken-Granitz		
Land:	Deutschland		
URL:			

Teil 1b. Informationen zur Firma des Qualified Security Assessors (falls vorhanden)			
Firmenname:			
Name Leiter QSA:		Titel:	
Telefon:		E-Mail:	
Geschäftsadresse:			
Land:			
URL:			

Teil 2. Zusammenfassung für die Geschäftsleitung

Teil 2a. Handelstätigkeit (alle zutreffenden Optionen auswählen)

☐ Einzelhändler	☐ Telekommunikation	☐ Lebensmitteleinzelhandel und Supermärkte
☐ Erdöl/Erdgas	☐ eCommerce	☐ Schriftliche/Telefonische Bestellung (MOTO)
☐ Sonstige (bitte angeben):		

Welche Zahlungskanäle bietet Ihr Unternehmen an?	Welche Zahlungskanäle werden durch diesen SBF abgedeckt?
☐ Schriftliche/Telefonische Bestellung (MOTO)	☐ Schriftliche/Telefonische Bestellung (MOTO)
☐ eCommerce	☐ eCommerce
☒ Vorlage der Karte (persönlich)	☒ Vorlage der Karte (persönlich)

Hinweis: Wird einer Ihrer Zahlungskanäle oder -prozesse durch diesen SBF nicht abgedeckt, wenden Sie sich bezüglich der Validierung für die anderen Kanäle an Ihren Acquirer oder Ihre Zahlungsmarke.

Teil 2b. Beschreibung des Zahlungskartengeschäfts

Wie und in welchem Ausmaß speichert, verarbeitet und/oder überträgt Ihr Unternehmen Karteninhaberdaten?	

Teil 2c. Standorte

Im PCI DSS-Bericht enthaltene Art der Einrichtung (z. B. Verkaufsstellen, Firmenbüros, Rechenzentren, Call-Center usw.) und eine Zusammenfassung der im PCI DSS-Bericht enthaltenen Standorte auflisten

Art der Einrichtung	Zahl der Einrichtungen dieser Art	Ort(e) der Einrichtung (Stadt, Land)

Teil 2d. Zahlungsanwendung

Nutzt das Unternehmen eine oder mehrere Zahlungsanwendungen? ☐ Ja ☒ Nein

Geben Sie folgende Informationen bezüglich der Zahlungsanwendungen an, die in Ihrem Unternehmen genutzt werden:

Zahlungsanwendungsname	Versionsnummer	Ablaufdatum PA-DSS-Verzeichnis (falls vorhanden)	Ist die Anwendung PA-DSS gelistet?	Ablaufdatum der PA-DSS-Liste (falls zutreffend)
			☐ Ja ☐ Nein	

Teil 2e. Beschreibung der Umgebung

Beschreiben Sie in **allgemeiner** Form die in dieser Beurteilung berücksichtigte Umgebung. Beispiel: • Ein- und ausgehende Verbindungen zur/von der CDE (cardholder data environment, Karteninhaberdaten-Umgebung). • Wichtige Systemkomponenten in der CDE, etwa POS-Geräte, Datenbanken und Webserver sowie weitere notwendige Zahlungskomponenten (falls zutreffend).	
Nutzt Ihr Unternehmen die Netzwerksegmentierung auf eine Weise, dass der Umfang Ihrer PCI-DSS-Umgebung davon betroffen ist? (Hinweise zur Netzwerksegmentierung finden Sie im PCI DSS im Abschnitt "Netzwerksegmentierung".)	☒ Ja ☐ Nein

Teil 2f. Drittanbieter	
Nutzt Ihr Unternehmen einen Qualified Integrator & Reseller (QIR)? Falls ja: Name des QIR-Unternehmens: QIR-Personenname: Beschreibung der vom QIR erbrachten Dienstleistungen:	[ ] Ja [x] Nein
Werden Karteninhaberdaten von Ihrem Unternehmen an externe Dienstanbieter (beispielsweise Qualified Integrator Resellers (QIR), Gateways, Zahlungsabwickler, Zahlungsdienstleister (PSP), Webhosting-Unternehmen, Flugreiseagenturen, Anbieter von Kundenbindungsprogrammen usw.) weitergegeben?	[x] Ja [ ] Nein

Falls ja:	
Name des Dienstanbieters:	**Beschreibung der erbrachten Dienstleistungen:**
DataCash	Ihr Anbieter für virtuelle Terminals

Hinweis: Anforderung 12.8 gilt für alle Stellen in dieser Liste.

Teil 2g. Qualifikation zum Ausfüllen des SBF C-VT

Der Händler bestätigt die Qualifikation zum Ausfüllen dieser Kurzfassung des Selbstbeurteilungsfragebogens (in Bezug auf diesen Zahlungskanal) aus folgenden Gründen:

[x]	Die Zahlungsabwicklung des Händlers erfolgt ausschließlich über ein virtuelles Zahlungsterminal, auf das über einen mit dem Internet verbundenen Webbrowser zugegriffen wird.
[x]	Die virtuelle Zahlungsterminallösung des Händlers wird von einem PCI-DSS-validierten Drittanbieter bereitgestellt und gehostet.
[x]	Der Zugriff des Händlers auf die PCI-DSS-konforme virtuelle Terminallösung erfolgt über einen Computer, der sich an einem einzelnen isolierten Standort befindet und nicht mit anderen Standorten oder Systemen innerhalb der Händlerumgebung verbunden ist.
[x]	Auf dem Computer des Händlers ist keine Software installiert, die die Speicherung von Karteninhaberdaten bewirkt (beispielsweise Software für Stapelverarbeitung oder Teilstreckenverfahren).
[x]	Am Computer des Händlers sind keine Hardwaregeräte zur Erfassung oder Speicherung von Karteninhaberdaten angeschlossen (beispielsweise Kartenleser).
[x]	Der Händler empfängt oder überträgt keinerlei Karteninhaberdaten anderweitig auf elektronischem Wege (beispielsweise über ein internes Netzwerk oder das Internet).
[x]	Der Händler speichert keine Karteninhaberdaten in elektronischer Form **und**
[x]	falls der Händler Karteninhaberdaten speichert, geschieht dies ausschließlich in Papierform oder als Kopie von Papierbelegen und nicht in elektronischer Form.

Abschnitt: Selbstbewertungsfragebogen C-VT

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

Selbstbeurteilung abgeschlossen am: 05/03/2023

Erstellung und Wartung sicherer Netzwerke und Systeme

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

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
1.2	Schränken die Firewall- und Router-Konfigurationen die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und sämtlichen Systemen in der Karteninhaberdaten-Umgebung wie folgt ein? ***Hinweis**: Ein "nicht vertrauenswürdiges Netzwerk" ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.*				
1.2.1 (a)	Ist der ein- und ausgehende Netzwerkverkehr auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Verkehr beschränkt?	☑	☐	☐	☐
1.2.1 (b)	Wird der restliche ein- und ausgehende Verkehr eigens abgelehnt (z. B. durch die Verwendung einer ausdrücklichen "Alle ablehnen"-Anweisung oder einer impliziten Anweisung zum Ablehnen nach dem Zulassen)?	☑	☐	☐	☐
1.2.3	Sind Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der CDE und Konfigurieren dieser Firewalls installiert und so konfiguriert, dass der gesamte Verkehr zwischen der drahtlosen Umgebung und der CDE abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt?	☑	☐	☐	☐
1.3	Verbietet die Firewall-Konfiguration wie folgt den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung?				
1.3.4	Ist die Weiterleitung ausgehenden Datenverkehrs von der Karteninhaberdaten-Umgebung an das Internet ausdrücklich erlaubt?	☑	☐	☐	☐
1.3.5	Sind nur etablierte Verbindungen in das Netzwerk zulässig?	☑	☐	☐	☐
1.4(a)	Ist eine persönliche Firewall-Software auf allen mobilen und/oder den Mitarbeitern gehörenden Geräten installiert, die außerhalb des Netzwerks auf das Internet zugreifen (z. B. Laptops, die von Mitarbeitern verwendet werden) und die auch für den Zugriff auf das Netzwerk eingesetzt werden?	☑	☐	☐	☐
1.4(b)	Ist die persönliche Firewall-Software gemäß spezifischen Konfigurationseinstellungen konfiguriert, wird sie aktiv ausgeführt und ist sie nicht durch Benutzer mobiler und/oder mitarbeitereigener Geräte veränderbar?	☑	☐	☐	☐

Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
2.1(a)	Werden vom Anbieter gelieferte Standardeinstellungen immer geändert, bevor ein System im Netzwerk installiert wird? *Dies gilt für SÄMTLICHE Standardkennwörter, wie etwa die von Betriebssystemen, Sicherheitssoftware, Anwendungs-und Systemkonten, POS (Point of Sale, Verkaufsstelle)-Terminals, Zahlungsanwendungeb, SNMP (Simple Network Management Protocol)-Community-Zeichenfolgen usw.).*	☑	☐	☐	☐
2.1(b)	Werden unnötige Standardkonten vor der Installation eines Systems im Netzwerk entfernt oder deaktiviert?	☑	☐	☐	☐
2.1.1	Für drahtlose Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder die Karteninhaberdaten übertragen, werden ALLE Standardeinstellungen des Wireless-Anbieters wie folgt geändert?				
2.1.1 (a)	Werden Standardwerte der Verschlüsselungsschlüssel zum Zeitpunkt der Installation geändert und werden sie jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt?	☑	☐	☐	☐
2.1.1 (b)	Werden Standard-SNMP-Community-Zeichenfolgen auf kabellosen Geräten bei der Installation geändert?	☑	☐	☐	☐
2.1.1 (c)	Werden Standardkennwörter/-sätze auf Zugriffspunkten bei der Installation geändert?	☑	☐	☐	☐
2.1.1 (d)	Wird die Firmware auf drahtlosen Geräten aktualisiert, um eine starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen?	☑	☐	☐	☐
2.1.1 (e)	Werden gegebenenfalls auch andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen geändert?	☑	☐	☐	☐
2.2.2 (a)	Werden für den Betrieb des Systems nur notwendige Dienste, Protokolle, Daemons usw. aktiviert (d. h. nicht direkt für die Ausführung der spezifischen Gerätefunktion erforderliche Funktionen werden deaktiviert)?	☑	☐	☐	☐
2.2.2 (b)	Sind alle aktivierten unsicheren Dienste, Daemons oder Protokolle durch die dokumentierten Konfigurationsstandards legitimiert?	☑	☐	☐	☐
2.2.3	Sind zusätzliche Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden, dokumentiert und implementiert? **Hinweis:** *Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 abgeschlossen werden.*	☑	☐	☐	☐
2.2.4 (a)	Verstehen sich Systemadministratoren und/oder Mitarbeiter, die Systemkomponenten konfigurieren, auf allgemeine Sicherheitsparametereinstellungen für diese Systemkomponenten?	☑	☐	☐	☐

2.2.4 (b)	Sind in den Systemkonfigurationsstandards gängige Sicherheitsparametereinstellungen enthalten?	☑	☐	☐	☐
2.2.4 (c)	Sind die Sicherheitsparametereinstellungen auf den Systemkomponenten sachgemäß eingestellt?	☑	☐	☐	☐
2.2.5 (a)	Wurden alle unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver entfernt?	☑	☐	☐	☐
2.2.5 (b)	Werden aktivierte Funktionen dokumentiert und sind sie sicher konfiguriert?	☑	☐	☐	☐
2.2.5 (c)	Sind auf den Systemkomponenten ausschließlich dokumentierte Funktionen vorhanden?	☑	☐	☐	☐
2.3	Ist der Nichtkonsolen-Verwaltungszugriff wie folgt verschlüsselt? **Hinweis:** *Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 abgeschlossen werden*				
2.3(a)	Werden alle Nichtkonsolen-Verwaltungszugriffe mit einer starken Kryptographie verschlüsselt und wird eine starke Verschlüsselungsmethode aufgerufen, bevor das Administratorkennwort angefordert wird?	☑	☐	☐	☐
2.3(b)	Sind die Systemdienste und -parameterdateien so konfiguriert, dass die Nutzung von Telnet und anderen unsicheren Remote-Anmeldebefehlen verhindert wird?	☑	☐	☐	☐
2.3(c)	Ist der Administratorzugriff auf die webbasierten Managementschnittstellen mit einer starken Kryptographie verschlüsselt?	☑	☐	☐	☐
2.3(d)	Wird für die eingesetzte Technologie eine starke Kryptographie gemäß den bewährten Branchenverfahren und/oder Anbieterempfehlungen implementiert?	☑	☐	☐	☐

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
3.2(c)	Werden vertrauliche Authentifizierungsdaten nach Abschluss des Autorisierungsprozesses so gelöscht, dass sie nicht wiederhergestellt werden können?	☑	☐	☐	☐
3.2(d)	Halten alle Systeme die folgenden Anforderungen hinsichtlich des Verbots, vertrauliche Authentifizierungsdaten nach der Autorisierung zu speichern, ein (auch wenn diese verschlüsselt sind)?				
3.2.2	Wird der Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte) nach der Autorisierung tatsächlich nicht gespeichert?	☑	☐	☐	☐
3.2.3	Wird die persönliche Identifizierungsnummer (PIN) oder der verschlüsselte PIN-Block nach der Autorisierung nicht gespeichert?	☑	☐	☐	☐
3.3	Wird die PAN zum Teil verborgen (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), sodass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können? ***Hinweis:*** *Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten - z. B. bei juristischen Anforderungen und Anforderungen der Kreditkartenunternehmen an POS-Belege.*	☑	☐	☐	☐

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

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
4.1(a)	Werden eine starke Kryptographie und Sicherheitsprotokolle eingesetzt, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen? ***Hinweis:*** *Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 abgeschlossen werden.* *Zu den offenen, öffentlichen Netzwerken gehören insbesondere das Internet, Drahtlostechnologien wie 802.11 und Bluetooth sowie Mobilfunktechnologien wie Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) und General Packet Radio Service (GPRS).*	☑	☐	☐	☐

4.1(b)	Werden ausschließlich vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert?	☑	☐	☐	☐
4.1(c)	Sind Sicherheitsprotokolle implementiert, um ausschließlich sichere Konfigurationen zu verwenden und keine unsicheren Versionen oder Konfigurationen zu unterstützen?	☑	☐	☐	☐
4.1(d)	Wird für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet (siehe Anbieterempfehlungen/bewährte Verfahren)?	☑	☐	☐	☐
4.1(e)	Wird bei TLS-Implementierungen bei jeder Übertragung bzw. bei jedem Empfang von Karteninhaberdaten TLS aktiviert? *Bei browserbasierten Implementierungen ist beispielsweise Folgendes zu prüfen:* • *Wird "HTTPS" als Bestandteil des Browser-URL-Protokolls angezeigt* • Werden Karteninhaberdaten nur angefordert, wenn die URL die Komponente "HTTPS" enthält?	☑	☐	☐	☐
4.1.1	Werden bewährte Branchenverfahren eingesetzt, um eine starke Verschlüsselung in der Authentifizierung und Übertragung für drahtlose Netzwerke zu implementieren, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind?	☑	☐	☐	☐
4.2(b)	Sind Richtlinien vorhanden, die festlegen, dass ungeschützte PANs nicht über Messaging-Technologien für Endanwender gesendet werden dürfen?	☑	☐	☐	☐

Unterhaltung eines Anfälligkeits-Managementprogramms

Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
5.1	Ist eine Antivirensoftware auf allen Systemen, die üblicherweise das Ziel böswilliger Software sind, implementiert?	☑	☐	☐	☐
5.1.1	Sind die Virenschutzprogramme in der Lage, bekannte Malware-Typen (z. B. Viren, Trojaner, Würmer, Spyware, Adware und Rootkits) zu erkennen, zu entfernen und vor ihnen zu schützen?	☑	☐	☐	☐
5.1.2	Wird bei Systemen, die in der Regel nicht von Malware befallen sind, regelmäßig geprüft, ob sich die Malware-Bedrohung erhöht hat und diese Systeme unverändert weiter genutzt werden können?	☑	☐	☐	☐
5.2	Es ist zu überprüfen, ob bei allen Antivirenmechanismen Folgendes beachtet wird:				
5.2(a)	Sind die Antivirensoftware und die Definitionen immer auf dem neuesten Stand?	☑	☐	☐	☐
5.2(b)	Sind automatische Updates und regelmäßige Scans aktiviert und werden sie regelmäßig durchgeführt?	☑	☐	☐	☐
5.2(c)	Generieren alle Virenschutzmechanismen Prüfprotokolle und werden die Protokolle gemäß PCI-DSS-Anforderung 10.7 aufbewahrt?	☑	☐	☐	☐
5.3	Aspekte bei Antivirenmechanismen: • Werden alle Antivirenmechanismen aktiv ausgeführt? • Sind sie gegen benutzerseitige Deaktivierungen oder Veränderungen gesichert? ***Hinweis:*** *Antivirenlösungen können nur dann vorübergehend deaktiviert werden, wenn es einen triftigen technischen Grund dafür gibt. Dieser muss vom Management fallweise autorisiert werden. Wenn der Virenschutz aus bestimmten Gründen deaktiviert werden muss, ist hierfür eine förmliche Autorisierung erforderlich. Zusätzliche Sicherheitsmaßnahmen müssen auch für den Zeitraum, in dem der Virenschutz nicht aktiv ist, getroffen werden.*	☑	☐	☐	☐

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

PCI-DSS-Frage	Antwort: (je Frage eine Antwort markieren)			
	Ja	Ja, mit CCW	Nein	Nicht zutr.

6.1	Gibt es einen Prozess zur Erkennung folgender und anderer Sicherheitsrisiken? • Nutzung verlässlicher externer Informationsquellen • Zuweisung von Risikostufen für Sicherheitsrisiken mit der Ermittlung sämtlicher "hohen" und "kritischen" Risiken ***Hinweis:*** *Die Risikostufen sollten auf den bewährten Verfahren der Branche beruhen und die potenziellen Auswirkungen berücksichtigen. So könnten der CVSS-Basiswert und/oder die Klassifizierung durch den Anbieter sowie die Art der betroffenen Systeme als Kriterien für die Einteilung der Sicherheitsrisiken in verschiedene Stufen dienen.* *Die Methoden zur Bewertung der Sicherheitsrisiken und zur Einteilung in Sicherheitsstufen hängen von der Unternehmensumgebung und der Strategie zur Risikobewertung ab. Bei der Risikoeinstufung müssen zumindest die Sicherheitsrisiken ermittelt werden, die als "hohes Risiko" für die Umgebung gelten. Zusätzlich zu der Risikoeinstufung können einzelne Sicherheitsrisiken als "kritisch" betrachtet werden, falls sie eine unmittelbare Bedrohung der Umgebung darstellen, sich auf wichtige Systeme auswirken und/oder eine potenzielle Gefährdung darstellen, wenn nicht auf sie eingegangen wird. Beispiele für wichtige Systeme sind Sicherheitssysteme, öffentlich zugängliche Geräte und Systeme, Datenbanken und andere Systeme, in denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden.*	☑	☐	☐	☐
6.2(a)	Sind alle Systemkomponenten und Softwareanwendungen mithilfe der neuesten Sicherheitspatches des jeweiligen Anbieters vor bekannten Sicherheitsrisiken geschützt?	☑	☐	☐	☐
6.2(b)	Werden wichtige Sicherheitspatches innerhalb eines Monats nach der Freigabe installiert? ***Hinweis:*** *Kritische Sicherheitspatches müssen gemäß dem in Anforderung 6.1 festgelegten Prozess zur Risikoeinstufung ermittelt werden.*	☑	☐	☐	☐

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
7.1	Ist der Zugriff auf Systemkomponenten und Karteninhaberdaten wie folgt ausschließlich auf jene Personen beschränkt, deren Tätigkeit diesen Zugriff erfordert?				
7.1.2	Ist der Zugriff auf privilegierte Benutzer-IDs wie folgt beschränkt? • Auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind Exklusive Zuweisung zu Rollen, die diesen privilegierten Zugriff konkret benötigen	☑	☐	☐	☐
7.1.3	Werden Zugriffsberechtigungen anhand der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter zugewiesen?	☑	☐	☐	☐

Anforderung 8: Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
8.1.1	Wurde allen Benutzern eine eindeutige ID zugewiesen, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wurde?	☑	☐	☐	☐
8.1.3	Wird der Zugriff ehemaliger Benutzer sofort deaktiviert oder entfernt?	☑	☐	☐	☐
8.2	Werden neben der Zuweisung einer eindeutigen ID eine oder mehrere der folgenden Methoden eingesetzt, um alle Benutzer zu authentifizieren? • Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; • etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; • etwas, das Sie sind, wie zum Beispiel biometrische Daten.	☑	☐	☐	☐
8.2.3 (a)	Sind Parameter für Benutzerkennwörter so konfiguriert, dass die Kennwörter/-sätze folgende Voraussetzungen erfüllen müssen? • Kennwörter müssen mindestens sieben Zeichen umfassen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden. Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.	☑	☐	☐	☐

8.3	Sind der gesamte Nicht-Konsolenverwaltungszugriff durch Einzelpersonen und der gesamte Remotezugriff auf die CDE mittels Mehrfaktorenauthentifizierung wie folgt geschützt? ***Hinweis:*** *Für die Mehrfaktorenauthentifizierung ist es erforderlich, dass mindestens zwei von drei Authentifizierungsmethoden (Beschreibungen der Authentifizierungsmethoden finden Sie unter "PCI DSS Requirement 8.2") für die Authentifizierung verwendet werden. Die doppelte Verwendung eines Faktors (beispielsweise durch die Verwendung von zwei separaten Passwörtern) wird nicht als Mehrfaktorenauthentifizierung erachtet.*				
8.3.1	Ist die Multi-Faktor-Authentifizierung fester Bestandteil für alle Nichtkonsolen-Zugriffe auf das CDE durch Mitarbeiter mit Verwaltungszugriff?	☑	☐	☐	☐
8.5	Sind Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden wie folgt untersagt? • Allgemeine Benutzer-IDs und -konten wurden deaktiviert oder entfernt; • es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen; und • es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.	☑	☐	☐	☐

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
9.1	Wird der Zugang zu sensiblen Bereichen entweder mithilfe von Videokameras und /oder Kontrollsystemen (oder beidem) überwacht? ***Hinweis:*** *"Zugangsbeschränkte Bereiche" sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die öffentlichen Bereiche, in denen lediglich POS-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).*	☑	☐	☐	☐
9.5	Wird die physische Sicherheit aller Medien gewährleistet (insbesondere Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)? *Zum Zwecke der Anforderung 9 bezieht sich der Begriff "Medien" auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.*	☑	☐	☐	☐
9.6(a)	Wird die interne oder externe Verteilung jeglicher Art von Medien stets strikt kontrolliert?	☑	☐	☐	☐
9.6(b)	Umfassen die Kontrollen folgende Punkte?				
9.6.1	Werden Medien klassifiziert, sodass die Sensibilität der Daten bestimmt werden kann?	☑	☐	☐	☐

9.6.2	Werden Medien über einen sicheren Kurier oder andere Liefermethoden gesendet, die eine genaue Verfolgung der Sendung erlauben?	☑	☐	☐	☐
9.6.3	Wird vor dem Verlagern von Medien die Genehmigung des Managements eingeholt (insbesondere wenn Medien an Einzelpersonen verteilt werden)?	☑	☐	☐	☐
9.7	Werden strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durchgeführt?	☑	☐	☐	☐
9.8(a)	Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?	☑	☐	☐	☐
9.8(c)	Erfolgt die Vernichtung von Medien wie nachstehend beschrieben?				
9.8.1 (a)	Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?	☑	☐	☐	☐
9.8.1 (b)	Werden Container zur Aufbewahrung von zu vernichtenden Informationen so geschützt, dass Zugriffe auf diese Inhalte vermieden werden?	☑	☐	☐	☐

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
11.3.4	Falls die CDE durch Segmentierung von anderen Netzwerken isoliert wird:				
11.3.4 (a)	Sehen die Penetrationstestverfahren vor, dass alle Segmentierungsmethoden daraufhin geprüft werden, ob sie funktionieren und effektiv sind, und dass alle Systeme außerhalb des Bereichs von den Systemen innerhalb des CDE isoliert werden müssen?	☑	☐	☐	☐
11.3.4 (b)	Erfüllen die Penetrationstests zur Überprüfung der Segmentierungskontrollen die folgenden Voraussetzungen? • Die Tests werden mindestens einmal jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt. • Bei den Tests werden alle angewendeten Segmentierungskontrollen/-methoden geprüft. • Es wird geprüft, ob die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden.	☑	☐	☐	☐
11.3.4 (c)	Werden die Tests von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt und ist der Tester gegebenenfalls für eine unabhängige Organisation tätig (muss kein QSA oder ASV sein)?	☑	☐	☐	☐

Befolgung einer Informationssicherheitsrichtlinie

Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.

Hinweis: Zum Zwecke der Anforderung 12 bezieht sich der Begriff "Mitarbeiter" hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Stelle "ansässig" sind oder anderweitig Zugriff auf die Karteninhaberdaten-Umgebung haben.

PCI-DSS-Frage		Antwort: (je Frage eine Antwort markieren)			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
12.1	Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und an das betroffene Personal weitergeleitet?	☑	☐	☐	☐
12.1.1	Wird die Sicherheitsrichtlinie mindestens einmal pro Jahr überarbeitet und bei Umgebungsänderungen aktualisiert?	☑	☐	☐	☐
12.3	Wurden Nutzungsrichtlinien für wichtige Technologien entwickelt, um die ordnungsgemäße Nutzung dieser Technologien zu regeln - unter Berücksichtigung der nachfolgenden Punkte? ***Hinweis:*** *Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.*				
12.3.1	Ausdrückliche Genehmigung durch autorisierte Parteien, diese Technologien zu nutzen	☑	☐	☐	☐
12.3.3	Eine Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	☑	☐	☐	☐
12.3.5	Akzeptable Nutzung dieser Technologien	☑	☐	☐	☐
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	☑	☐	☐	☐
12.5 (b)	Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?				
12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?	☑	☐	☐	☐
12.6(a)	Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheitheitsrichtlinien und Verfahren der Karteninhaberdaten zu vermitteln?	☑	☐	☐	☐
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert und gepflegt?				
12.8.1	Wird eine Liste von Dienstanbietern mit Angabe einer Beschreibung der geleisteten Dienstleistung gepflegt?	☑	☐	☐	☐

12.8.2	Wird eine schriftliche Vereinbarung aufbewahrt, mit der bestätigt wird, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden bzw. die er für den Kunden speichert, verarbeitet oder überträgt, oder dass die Sicherheit der CDE betroffen sein könnte. ***Hinweis:*** *Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.*	☑	☐	☐	☐
12.8.3	Gibt es ein eindeutiges Verfahren für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht?	☑	☐	☐	☐
12.8.4	Gibt es ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard?	☑	☐	☐	☐
12.8.5	Werden Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden, aufbewahrt?	☑	☐	☐	☐
12.10.1 (a)	Wurde ein Vorfallreaktionsplan erstellt, der im Falle einer Systemsicherheitsverletzung im System implementiert wird?	☑	☐	☐	☐

Anhang A: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsamem Hosting

Dieser Anhang wird nicht für Händlerbeurteilungen verwendet.

Anhang B: Arbeitsblatt - Kompensationskontrollen

Bestimmen Sie anhand dieses Arbeitsblatts die Kompensationskontrollen für alle Anforderungen, bei denen "Ja, mit CCW" markiert wurde.

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.

Informationen zu Kompensationskontrollen sowie Hinweise zum Ausfüllen dieses Arbeitsblatts finden Sie in den PCI-DSS-Anhängen B, C und D.

Anforderungsnummer und -definition:

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

Anhang C: Erläuterung der Nichtanwendbarkeit

Falls die Spalte "N/A" (Nicht zutreffend) im Fragebogen markiert wurde, erläutern Sie bitte im Arbeitsblatt, warum die zugehörige Anforderung nicht für Ihr Unternehmen gilt.

Anforderung	Grund, warum die Anforderung nicht anwendbar ist.

Vermerk

MIDs/Konten, die von dieser Konformitätsbescheinigung abgedeckt sind

MID/Konto	Firmenname	Adresszeile 1
803642751	Hohmann Weinbau Rügen GmbH	DorstraBe 16 16, 18586, Lancken-Granitz

Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

Auf der Grundlage der Ergebnisse des SBF C-VT vom (Abschlussdatum) stellen die in Teil 3b bis 3d angegebenen Unterzeichner den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom 05/03/2023 ermittelte Stelle fest: **(eine Option angeben)** :

☒	**Konform:** Alle Abschnitte des PCI DSS SBF sind vollständig und alle Fragen wurden mit "Ja" beantwortet. Daraus ergibt sich die Gesamtbewertung **KONFORM**. Hohmann Weinbau Rügen GmbH hat somit vollständig Konformität mit dem PCI DSS gezeigt.
☐	**Nicht konform:** Nicht alle Abschnitte des PCI DSS SBF sind vollständig und/oder nicht alle Fragen wurden mit "Ja" beantwortet. Daraus ergibt sich die Gesamtbewertung **NICHT KONFORM**. Hohmann Weinbau Rügen GmbH hat somit nicht vollständige Konformität mit dem PCI DSS gezeigt. **Zieldatum für Konformität:** Eine Stelle, die dieses Formular mit dem Status "Nicht konform" einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen.
☐	**Konform, jedoch mit gesetzlicher Ausnahme:** Eine oder mehrere Anforderungen sind aufgrund einer gesetzlichen Einschränkung, die das Erfüllen der jeweiligen Anforderung(en) unmöglich macht, mit "Nein" gekennzeichnet. Bei dieser Option ist eine zusätzliche Prüfung durch den Acquirer oder die Zahlungsmarke erforderlich.

Teil 3a. Feststellung des Status

Unterzeichner bestätigt:
(Zutreffendes ankreuzen)

x	Der PCI-DSS-Selbstbeurteilungsfragebogen C-VT, Version 3.2.1, wurde den enthaltenen Anleitungen gemäß ausgefüllt.
x	Alle Angaben im oben genannten SBF und in dieser Bescheinigung vermitteln ein in jeder Hinsicht den tatsächlichen Verhältnissen entsprechendes Bild von den Ergebnissen meiner Beurteilung.
x	Ich habe den PCI DSS gelesen und erkenne an, dass ich jederzeit die für meine Umgebung geltende PCI-DSS-Konformität aufrechterhalten muss.
x	Für den Fall, dass sich meine Umgebung ändert, erkenne ich an, dass ich meine Umgebung erneut beurteilen und etwaige zusätzliche PCI-DSS-Anforderungen erfüllen muss.
x	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurden vollständige Spurdaten ("Full-Track-Daten")[1], CAV2-, CVC2-, CID-, CVV2[2]- oder PIN-Daten[3] gefunden.

Teil 3b. Bescheinigung des Händlers

Unterschrift des Beauftragten des Händlers Dies wurde von weingut_ruegen im Namen von Hohmann Weinbau Rügen GmbH elektronisch unterzeichnet.	*Datum:* 05/03/2023
Name des Beauftragten des Händlers: Simone Hantke	*Titel:* Frau

Teil 3c. QSA-Bestätigung (falls zutreffend)

Falls ein QSA an dieser Beurteilung beteiligt war, beschreiben Sie bitte dessen Aufgabe:	
Signatur des Bevollmächtigten des QSA-Unternehmens This was electronically signed by 803642751 on behalf of Hohmann Weinbau Rügen GmbH	*Datum:*
Name des Bevollmächtigten:	*Unternehmen des QSA:*

Teil 3d. ISA-Bestätigung (falls zutreffend)	
Falls ein ISA an dieser Beurteilung beteiligt war, beschreiben Sie bitte dessen Aufgabe:	
Unterschrift des ISA	*Datum:*
Name des ISA:	*Titel:*

[1] Im Magnetstreifen verschlüsselte Daten oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Spurdaten speichern. Die einzigen Spurdatenelemente, die aufbewahrt werden dürfen, sind die primäre Kontonummer (PAN), das Ablaufdatum und der Name des Karteninhabers.

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

[3] Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.