



**Payment Card Industry (PCI)
Data Security Standard
Questionario di autovalutazione C-VT
e Attestato di conformità**

**Terminali virtuali basati su Web, nessuna
memorizzazione elettronica dei dati di titolari di
carta**

Versione 2.0

Ottobre 2010

Modifiche del documento

Data	Versione	Descrizione
28 ottobre 2010	2.0	Nuovo Questionario di autovalutazione e Attestato di conformità per esercenti che utilizzano solo terminali virtuali basati su Web. In linea con i requisiti e le procedure di test PCI DSS v2.0.

Sommario

Modifiche del documento	i
PCI DSS: Documenti correlati	iii
Operazioni preliminari	iv
Completamento del questionario di autovalutazione	iv
Conformità agli standard PCI DSS – Operazioni	v
Guida per la non applicabilità di determinati requisiti specifici.....	v
Attestato di conformità, SAQ C-VT	1
Questionario di autovalutazione C-VT.....	6
Sviluppo e gestione di una rete sicura	6
<i>Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta.....</i>	<i>6</i>
<i>Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione</i>	<i>7</i>
Protezione dei dati di titolari di carta.....	8
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati</i>	<i>8</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche</i>	<i>8</i>
Utilizzare un programma per la gestione delle vulnerabilità	9
<i>Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus.....</i>	<i>9</i>
<i>Requisito 6: Sviluppare e gestire sistemi e applicazioni protette</i>	<i>9</i>
Implementazione di rigide misure di controllo dell'accesso	10
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario..</i>	<i>10</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta</i>	<i>10</i>
Gestione di una politica di sicurezza delle informazioni	12
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale</i>	<i>12</i>
Appendice A: (non utilizzata)	14
Appendice B: Controlli compensativi.....	15
Appendice C: Foglio di lavoro - Controlli compensativi.....	17
Foglio di lavoro Controlli compensativi - Esempio	18
Appendice D: Spiegazione di non applicabilità.....	19

PCI DSS: Documenti correlati

I seguenti documenti sono stati creati per una migliore comprensione degli standard PCI DSS e dei questionari di autovalutazione appropriati da parte di esercenti e provider di servizi.

Documento	Destinatari
<i>PCI DSS: Requisiti e procedure di valutazione della sicurezza</i>	Tutti gli esercenti e i provider di servizi
<i>Navigazione in PCI DSS: Comprensione dello scopo dei requisiti</i>	Tutti gli esercenti e i provider di servizi
<i>PCI DSS: Istruzioni e linee guida per l'autovalutazione</i>	Tutti gli esercenti e i provider di servizi
<i>PCI DSS: Questionario di autovalutazione A e Attestato</i>	Esercenti idonei ¹
<i>PCI DSS: Questionario di autovalutazione B e Attestato</i>	Esercenti idonei ¹
<i>PCI DSS: Questionario di autovalutazione C-VT e Attestato</i>	Esercenti idonei ¹
<i>PCI DSS: Questionario di autovalutazione C e Attestato</i>	Esercenti idonei ¹
<i>PCI DSS: Questionario di autovalutazione D e Attestato</i>	Esercenti e provider di servizi idonei ¹
<i>PCI Data Security Standard e Payment Application Data Security Standard: Glossario, abbreviazioni e acronimi</i>	Tutti gli esercenti e i provider di servizi

¹ Per determinare il questionario di autovalutazione appropriato, fare riferimento al documento *PCI DSS: Istruzioni e linee guida per l'autovalutazione*, "Scelta del questionario SAQ e dell'attestato più appropriati per la propria azienda".

Operazioni preliminari

Completamento del questionario di autovalutazione

Il questionario SAQ C-VT è stato sviluppato per rispondere ai requisiti applicabili a tutti gli esercenti che elaborano i dati dei titolari di carta solo mediante terminali virtuali isolati su computer connessi a Internet.

Un terminale virtuale è un accesso basato su browser Web al sito Web di un acquirente, elaboratore o provider di servizi di terzi per autorizzare le transazioni della carta di pagamento, in cui l'esercente inserisce manualmente i dati della carta mediante un browser Web connesso in modo sicuro. A differenza dei terminali fisici, quelli virtuali non leggono i dati direttamente da una carta di pagamento. Dal momento che le transazioni della carta di pagamento sono inserite manualmente, i terminali virtuali sono in genere usati al posto dei terminali fisici in ambienti di esercenti con un volumi limitati di transazioni.

Questi esercenti elaborano i dati dei titolari di carta solo tramite un terminale virtuale e non memorizzano tali dati su alcun computer. Questi terminali virtuali sono connessi a Internet per accedere a terze parti che ospitano la funzione di elaborazione del pagamento del terminale virtuale. Questa terza parte può essere un elaboratore, un acquirente o un altro provider di servizi di terzi che memorizza, elabora e/o trasmette i dati dei titolari di carta per autorizzare e/o contabilizzare le transazioni di pagamento del terminale virtuale dell'esercente.

L'applicazione di questa opzione SAQ riguarda solo gli esercenti che inseriscono manualmente una singola transazione alla volta con una tastiera in una soluzione di terminale virtuale basato su Web.

Gli esercenti SAQ C-VT elaborano i dati dei titolari di carta utilizzando terminali virtuali connessi a Internet, non memorizzano dati dei titolari di carta su alcun computer e possono essere esercenti con punti vendita reali (carta presente) oppure esercenti con vendita per posta/telefono (carta non presente). Tali esercenti devono convalidare la propria conformità completando il questionario SAQ C-VT e l'attestato di conformità ad esso associato, confermando che:

- L'unica elaborazione di pagamenti della società viene effettuata mediante un terminale virtuale a cui si accede mediante un browser Web collegato ad Internet.
- La soluzione di terminale virtuale della società è fornita ed ospitata da un provider di servizi di terze parti convalidato PCI DSS.
- La società accede alla soluzione di terminale virtuale conforme PCI DSS via computer ed è isolata in un'unica posizione e non è collegata ad altre posizioni o sistemi all'interno del suo ambiente (ciò si può ottenere mediante segmentazione di rete o firewall per isolare il computer dagli altri sistemi).
- Sul computer della società non è installato alcun software che determina la memorizzazione dei dati dei titolari di carta (ad esempio, non vi è alcun software per elaborazione batch o store-and-forward).
- Il computer della società non dispone di alcun dispositivo hardware collegato che viene usato per acquisire o memorizzare i dati dei titolari di carta (ad esempio non sono collegati lettori di carte).
- La società non riceve o trasmette in altro modo i dati dei titolari di carta elettronicamente tramite alcun canale (ad esempio mediante una rete interna o Internet).
- La società conserva solo resoconti o copie cartacee delle ricevute.
- La società non memorizza i dati di titolari di carta in formato elettronico.

Questa opzione non si applica mai alle società di e-commerce.

Ciascuna sezione del questionario riguarda un'area di sicurezza specifica, in base ai requisiti degli *standard di sicurezza dei dati PCI e le procedure di valutazione della sicurezza*. Questa versione più breve del questionario di autovalutazione comprende domande che riguardano un tipo specifico di ambiente di esercenti di dimensioni ridotte, secondo quanto definito nei criteri di idoneità esposti in precedenza. Qualora siano presenti requisiti PCI DSS applicabili al proprio ambiente che non sono coperti dal presente questionario di autovalutazione, ciò potrebbe indicare che questo questionario non è adatto al proprio ambiente. Inoltre, è tuttavia necessario soddisfare tutti i requisiti PCI DSS applicabili per garantire la conformità agli standard PCI DSS.

Conformità agli standard PCI DSS – Operazioni

1. Valutare il proprio ambiente per la conformità agli standard PCI DSS.
2. Completare il questionario di autovalutazione (SAQ C-VT) in base alle istruzioni contenute nel documento *Istruzioni e linee guida per l'autovalutazione*.
3. Completare per intero l'attestato di conformità.
4. Inviare il questionario SAQ e l'attestato di conformità, insieme ad eventuale altra documentazione richiesta, al proprio acquirente.

Guida per la non applicabilità di determinati requisiti specifici

Esclusione: Se per convalidare la propria conformità agli standard PCI DSS occorre completare il questionario SAQ C-VT, è possibile considerare la seguente eccezione: Vedere "Non applicabilità" di seguito per la risposta appropriata al questionario SAQ.

- Fornire una risposta alle domande specifiche della tecnologia wireless solo se tale tecnologia è disponibile nella propria rete (ad esempio, requisito 2.1.1).

Non applicabilità: questo ed eventuali altri requisiti considerati non applicabili al proprio ambiente devono essere indicati con "N/A" nella colonna "Speciale" del questionario SAQ. Di conseguenza, completare il foglio di lavoro "Spiegazione di non applicabilità" nell'appendice D per ogni voce "N/A".

Attestato di conformità, SAQ C-VT

Istruzioni per l'invio

L'esercente deve completare questo Attestato di conformità come una dichiarazione del proprio stato di conformità agli *Standard di protezione dei dati per il settore delle carte di pagamento (PCI DSS)* e alle procedure di valutazione della sicurezza. Completare tutte le sezioni applicabili e fare riferimento alle istruzioni per l'invio nella sezione "Conformità agli standard PCI DSS - Operazioni" nel presente documento.

Parte 1. Informazioni Esercente e azienda qualificata per la valutazione (QSA)

Parte 1a. Informazioni sull'organizzazione dell'esercente

Ragione sociale:		DBA:	
Nome referente:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP:
URL:			

Parte 1b. Informazioni sull'azienda qualificata per la valutazione (se applicabile)

Ragione sociale:			
Nome referente QSA principale:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP:
URL:			

Parte 2. Tipo di esercente (selezionare tutte le risposte applicabili):

- Rivenditore
 Telecomunicazioni
 Negozi di alimentari e supermercati
 Distributori di benzina
 Ordini via posta/telefono
 Altro (specificare):

Elencare le strutture e le posizioni incluse nella valutazione della conformità agli standard PCI DSS:

Parte 2a. Rapporti

La società ha rapporti con uno o più agenti di terze parti (ad esempio gateway, società di hosting Web, addetti alle prenotazioni aeree, agenti di programmi di fedeltà, ecc.)? Sì No

La società ha rapporti con più di un acquirente? Sì No

Parte 2b. Elaborazione delle transazioni

Fornire le seguenti informazioni in ordine alla soluzione di terminale virtuale utilizzata dalla propria azienda:

<u>Nome del Provider di servizi della soluzione terminale virtuale</u>	<u>Nome della soluzione terminale virtuale</u>	<u>Data dell'ultima convalida di conformità agli standard PCI DSS del Provider di servizi di terminale virtuale</u>

Parte 2c. Idoneità al completamento del modulo SAQ C-VT

L'esercente dichiara la propria idoneità per il completamento di questa versione più breve del questionario di autovalutazione, perché:

<input type="checkbox"/>	L'unica elaborazione di pagamenti dell'esercente viene effettuata mediante un terminale virtuale a cui si accede mediante un browser Web collegato ad Internet.
<input type="checkbox"/>	L'esercente accede al terminale virtuale tramite un computer che è isolato in una posizione unica e non è collegato ad altre posizioni o sistemi all'interno del proprio ambiente.
<input type="checkbox"/>	La soluzione di terminale virtuale dell'esercente è fornita ed ospitata da un provider di servizi di terze parti convalidato PCI DSS.
<input type="checkbox"/>	Il computer dell'esercente non dispone di software installato che determina la memorizzazione dei dati dei titolari di carta (ad esempio, non vi è alcun software per elaborazione batch o store-and-forward).
<input type="checkbox"/>	Il computer dell'esercente non dispone di alcun dispositivo hardware collegato usato per acquisire o memorizzare i dati dei titolari di carta (ad esempio non è collegato alcun lettore di carte).
<input type="checkbox"/>	L'esercente non riceve o trasmette in altro modo i dati dei titolari di carta elettronicamente tramite alcun canale (ad esempio mediante una rete interna o Internet).
<input type="checkbox"/>	L'esercente non memorizza i dati dei titolari di carta in formato elettronico (ad esempio, tali dati non sono memorizzati in strumenti di marketing o vendita come CRM).
<input type="checkbox"/>	In caso di memorizzazione dei dati dei titolari di carta da parte dell'esercente, tali dati sono solo in forma di resoconti o copie di ricevute cartacee e non sono ricevuti in formato elettronico.

Parte 3. Convalida PCI DSS

In base ai risultati del questionario SAQ C-VT datato (*data di compilazione*), (*ragione sociale esercente*) dichiara il seguente stato di conformità (selezionare una risposta):

- Conforme:** Tutte le sezioni del questionario SAQ PCI sono state completate e a tutte le domande è stato risposto "sì", determinando una valutazione di **CONFORMITÀ** globale; pertanto (*ragione sociale esercente*) ha dimostrato la massima conformità agli standard PCI DSS.

- Non conforme:** Non tutte le sezioni del questionario SAQ PCI sono state completate e ad alcune domande è stato risposto "no", determinando una valutazione di **NON CONFORMITÀ** globale; pertanto (*ragione sociale esercente*) non ha dimostrato la massima conformità agli standard PCI DSS.

Data di scadenza per conformità:

È possibile che a un'entità che invia questo modulo con lo stato 'Non conforme' venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. *Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

Parte 3a. Conferma dello stato di conformità

L'esercente conferma che:

<input type="checkbox"/>	Il questionario di autovalutazione C-VT PCI DSS, versione (<i>versione di SAQ</i>), è stato completato in base alle istruzioni qui fornite.
<input type="checkbox"/>	Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione sotto tutti gli aspetti.
<input type="checkbox"/>	Ho verificato con il fornitore dell'applicazione di pagamento che il mio sistema di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
<input type="checkbox"/>	Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard.
<input type="checkbox"/>	Nessuna prova di memorizzazione dei dati della striscia magnetica (traccia) ² , CAV2, CVC2, CID o CVV2 ³ oppure dei dati PIN ⁴ dopo l'autorizzazione della transazione è stata trovata sui sistemi controllati durante questa valutazione.

Parte 3b. Accettazione da parte dell'esercente

<i>Firma del funzionario esecutivo dell'esercente</i> ↑	<i>Data</i> ↑
<i>Nome funzionario esecutivo dell'esercente</i> ↑	<i>Mansione</i> ↑

Società esercente rappresentata ↑

² Dati codificati nella striscia magnetica o dati equivalenti su un chip utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare tutti i dati completi della striscia magnetica dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il numero cliente, la data di scadenza e il nome.

³ Il valore di tre o quattro cifre stampato nel riquadro della firma o a destra di questo riquadro oppure nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

⁴ Numero di identificazione personale inserito dal titolare della carta durante una transazione con carta presente e/o blocco PIN cifrato presente all'interno del messaggio di transazione.

Parte 4. Piano d'azione per lo stato di non conformità

Selezionare lo "Stato di conformità" appropriato per ciascun requisito. In caso di risposta negativa a uno dei requisiti, occorre specificare la data in cui la Società sarà conforme al requisito e una breve descrizione delle azioni che verranno intraprese per soddisfare il requisito. *Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

Requisito PCI DSS	Descrizione del requisito	Stato di conformità (selezionare una risposta)		Data e azioni di correzione (in caso di non conformità)
		SÌ	NO	
1	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati dei titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	<input type="checkbox"/>	<input type="checkbox"/>	
5	Utilizzare e aggiornare regolarmente il software antivirus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Sviluppare e gestire sistemi e applicazioni protette	<input type="checkbox"/>	<input type="checkbox"/>	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	<input type="checkbox"/>	<input type="checkbox"/>	

Questionario di autovalutazione C-VT

Nota: le domande seguenti sono numerate in base ai requisiti PCI DSS ed alle procedure di test, secondo quanto definito nel documento Requisiti PCI DSS e procedure di valutazione della sicurezza.

Data di completamento:

Sviluppo e gestione di una rete sicura

Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta

Domanda PCI DSS	Risposta:	Sì	No	Speciale*
1.2 Le configurazioni di firewall e router limitano le connessioni tra le reti non attendibili e qualsiasi sistema nell'ambiente dei dati di titolari di carta nel modo seguente: <i>Nota: una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.</i>				
1.2.1 (a) Il traffico in entrata e in uscita è limitato a quello necessario per l'ambiente dei dati di titolari di carta e le restrizioni sono documentate?	<input type="checkbox"/>	<input type="checkbox"/>		
(b) Il resto del traffico in entrata e in uscita è negato in modo specifico (ad esempio utilizzando un comando esplicito "deny all" o un comando implicito di negazione dopo un'istruzione "allow")?	<input type="checkbox"/>	<input type="checkbox"/>		
1.2.3 Sono installati i firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e tali firewall sono configurati per negare o controllare il traffico (se necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>		
1.3 La configurazione firewall vieta l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta, come segue:				
1.3.3 Sono stati vietati i percorsi diretti per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>		
1.3.5 È autorizzato in modo esplicito il traffico in uscita dall'ambiente dei dati di titolari di carta ad Internet?	<input type="checkbox"/>	<input type="checkbox"/>		
1.3.6 Un controllo efficiente, anche noto come "dynamic packet filtering" (ossia, che consente solo alle connessioni già "stabilite" di accedere alla rete), è stato implementato?	<input type="checkbox"/>	<input type="checkbox"/>		
1.4 (a) Il firewall personale (software) è installato e attivo su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale?	<input type="checkbox"/>	<input type="checkbox"/>		
(b) Il software del firewall personale è configurato in base a standard specifici ed in modo che non possa essere modificato da utenti di computer portatili e/o di proprietà dei dipendenti?	<input type="checkbox"/>	<input type="checkbox"/>		

Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione

Domanda PCI DSS		Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
2.1	I valori predefiniti del fornitore vengono sempre modificati prima di installare un sistema in rete? <i>Le impostazioni predefinite del fornitore comprendono, senza limitazione, password, stringhe di comunità SNMP (Simple Network Management Protocol) ed eliminazione di account non necessari.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, i valori predefiniti sono stati modificati come segue:				
	(a) Sono state modificate le chiavi di cifratura predefinite al momento dell'installazione e vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono state modificate le stringhe di comunità SNMP predefinite sui dispositivi wireless?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Sono state modificate le password/passphrase predefinite nei punti di accesso?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless?		<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	(a) Sono abilitati solo i servizi, protocolli, daemon ecc. necessari come richiesto per la funzione del sistema (sono disabilitati i servizi e protocolli che non sono strettamente necessari per eseguire la funzione specifica di un dispositivo)?		<input type="checkbox"/>	<input type="checkbox"/>	

Protezione dei dati di titolari di carta

Requisito 3: Proteggere i dati di titolari di carta memorizzati

Domanda PCI DSS	Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
3.2.2 Il codice o il valore di verifica della carta (numero di tre o quattro cifre impresso sulla parte anteriore o sul retro di una carta di pagamento) non viene memorizzato in alcun caso?		<input type="checkbox"/>	<input type="checkbox"/>	
3.3 Il PAN è mascherato quando visualizzato? (Non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) <i>Note:</i> <ul style="list-style-type: none"> ▪ questo requisito non si applica ai dipendenti e ad altre parti che hanno l'esigenza specifica di visualizzare il numero PAN intero. ▪ Questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati di titolari di carta, ad esempio per ricevute di punti di vendita (POS). 		<input type="checkbox"/>	<input type="checkbox"/>	

Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche

Domanda PCI DSS	Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
4.1 (a) Sono utilizzati i protocolli di crittografia e sicurezza avanzati, quali SSL/TLS, SSH o IPSEC, per proteggere i dati sensibili di titolari di carta durante la trasmissione su reti pubbliche e aperte? <i>Esempi di reti pubbliche aperte che rientrano nell'ambito degli standard PCI DSS comprendono, senza limitazioni, la rete Internet, le tecnologie wireless, le reti GSM (Global System for Mobile communications) e le reti GPRS (General Packet Radio Service).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Vengono accettati solo certificati e/o chiavi affidabili?		<input type="checkbox"/>	<input type="checkbox"/>	
(e) Per le implementazioni SSL/TLS: <ul style="list-style-type: none"> • L'HTTPS viene visualizzato come parte dell'URL del browser? • I dati del titolare di carta sono richiesti solo quando l'HTTPS viene visualizzato nell'URL? 		<input type="checkbox"/>	<input type="checkbox"/>	
4.2 (b) Sono presenti politiche in cui si indica che i PAN non protetti non si devono inviare mediante tecnologie di messaggistica degli utenti finali?		<input type="checkbox"/>	<input type="checkbox"/>	

Utilizzare un programma per la gestione delle vulnerabilità

Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus

Domanda PCI DSS		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale</u> *
5.1	È stato installato un programma antivirus su tutti i sistemi comunemente colpiti da malware?		<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Tutti i programmi antivirus sono in grado di rilevare, rimuovere e proteggere da tutti i tipi conosciuti di software dannoso (ad esempio virus, cavalli di Troia, worm, spyware, adware e rootkit)?		<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Tutti i software antivirus sono aggiornati, in esecuzione ed in grado di generare log di audit come segue:				
	(a) La politica antivirus richiede l'aggiornamento delle definizioni e del software antivirus?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Sono attivati aggiornamenti automatici e scansioni periodiche?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Tutti i meccanismi antivirus generano log di audit e, questi log sono conservati in base al Requisito 10.7 PCI DSS?		<input type="checkbox"/>	<input type="checkbox"/>	

Requisito 6: Sviluppare e gestire sistemi e applicazioni protette

Domanda PCI DSS		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale</u> *
6.1	(a) Tutti i componenti di sistema ed il software sono protetti dalle vulnerabilità note mediante l'installazione delle più recenti patch di sicurezza dei fornitori?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono state installate patch di protezione critiche entro un mese dal relativo rilascio?		<input type="checkbox"/>	<input type="checkbox"/>	

Implementazione di rigide misure di controllo dell'accesso

Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario

Domanda PCI DSS		Risposta:	Sì	No	Speciale *
7.1	L'accesso ai componenti di sistema e ai dati di titolari di carta è limitato solo alle persone per le cui mansioni è realmente necessario, come segue:				
7.1.1	I diritti di accesso per gli ID utente privilegiati sono limitati alla quantità minima necessaria per svolgere le responsabilità del ruolo?	<input type="checkbox"/>	<input type="checkbox"/>		
7.1.2	I privilegi sono assegnati a utenti singoli in base alla classificazione e alla funzione del relativo ruolo (anche noto come controllo dell'accesso basato su ruolo)?	<input type="checkbox"/>	<input type="checkbox"/>		

Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta

Domanda PCI DSS		Risposta:	Sì	No	Speciale *
9.6	Tutti i supporti sono protetti fisicamente (inclusi, senza limitazione, computer, supporti elettronici rimovibili, ricevute cartacee, resoconti cartacei e fax)? <i>Ai fini del Requisito 9, per "supporti" si intendono tutti i supporti elettronici e cartacei contenenti dati di titolari di carta.</i>	<input type="checkbox"/>	<input type="checkbox"/>		
9.7	(a) La distribuzione interna ed esterna di qualsiasi tipo di supporto è rigorosamente controllata?	<input type="checkbox"/>	<input type="checkbox"/>		
	(b) I controlli devono includere quanto segue:				
9.7.1	Il supporto è classificato in modo da poter determinare la sensibilità dei dati?	<input type="checkbox"/>	<input type="checkbox"/>		
9.7.2	Il supporto viene inviato tramite un corriere affidabile o un altro metodo di consegna che può essere adeguatamente monitorato?	<input type="checkbox"/>	<input type="checkbox"/>		
9.8	I registri sono conservati per rintracciare ogni supporto che viene spostato da un'area protetta e viene ottenuta l'approvazione del management prima di spostare i supporti (in particolare quando i supporti vengono distribuiti a singole persone)?	<input type="checkbox"/>	<input type="checkbox"/>		
9.9	Sono in atto controlli adeguati per la memorizzazione e l'accesso ai supporti?	<input type="checkbox"/>	<input type="checkbox"/>		

Domanda PCI DSS		Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
9.10	Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?		<input type="checkbox"/>	<input type="checkbox"/>	
La distruzione avviene in base alle seguenti modalità:					
9.10.1	(a) I materiali cartacei sono distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo da rendere impossibile la ricostruzione dei dati dei titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I contenitori usati per conservare le informazioni da distruggere sono protetti per impedire l'accesso al contenuto? (Ad esempio, un contenitore per "informazioni da distruggere" dispone di un dispositivo di blocco che impedisce l'accesso al contenuto).		<input type="checkbox"/>	<input type="checkbox"/>	

Gestione di una politica di sicurezza delle informazioni

Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale

Domanda PCI DSS		Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
12.1	È stata definita, pubblicata, gestita e diffusa una politica per la sicurezza tra tutto il personale interessato? <i>Ai fini del Requisito 12, per "personale" si intende un dipendente a tempo pieno o part-time, un dipendente con contratto a tempo determinato, un collaboratore o consulente che svolge le sue prestazioni in sede o che abbia in altro modo accesso all'ambiente dei dati dei titolari di carta della società.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	La politica di sicurezza delle informazioni viene rivista almeno una volta all'anno ed aggiornata per riflettere i cambiamenti agli obiettivi aziendali o all'ambiente a rischio?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Le politiche di uso per tecnologie critiche (ad esempio, tecnologie di accesso remoto, wireless, supporti elettronici rimovibili, laptop, tablet, PDA, uso della posta elettronica e di Internet) sono sviluppate per definire l'uso corretto di queste tecnologie per tutto il personale? E richiedono quanto segue:				
12.3.1	Approvazione esplicita delle parti autorizzate per l'uso delle tecnologie?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	Un elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Usi accettabili delle tecnologie?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	La politica e le procedure per la sicurezza definiscono chiaramente le responsabilità in termini di protezione delle informazioni per tutto il personale?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Le seguenti responsabilità per la gestione della sicurezza delle informazioni sono state assegnate a una singola persona o a un team?				
12.5.3	Definizione, documentazione e distribuzione di procedure di risposta ed escalation in caso di problemi di sicurezza per garantire una gestione tempestiva ed efficiente di tutte le situazioni?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	(a) È presente un programma formale di consapevolezza della sicurezza per rendere tutto il personale consapevole dell'importanza della sicurezza dei dati di titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
12.8	Se i dati di titolari di carta sono condivisi con provider di servizi, le politiche e le procedure per la gestione dei provider di servizi sono gestite e implementate come segue:				
12.8.1	È stato conservato un elenco di provider di servizi?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Viene conservato un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati di titolari di carta di cui entra in possesso?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Esiste un processo definito per incaricare i provider di servizi, che includa tutte le attività di dovuta diligenza appropriate prima dell'incarico?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Viene mantenuto un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi con cadenza almeno annuale?		<input type="checkbox"/>	<input type="checkbox"/>	

Appendice A: (non utilizzata)

Questa pagina è stata lasciata intenzionalmente vuota.

Appendice B: Controlli compensativi

È possibile adottare i controlli compensativi per la maggior parte dei requisiti PCI DSS, quando un'entità non è in grado di soddisfare un requisito nel modo esplicitamente richiesto, a causa di limitazioni aziendali tecniche o documentate legittime, ma ha posto in essere altri controlli (anche compensativi) sufficienti a mitigare il rischio associato a tale requisito.

I controlli compensativi devono soddisfare i seguenti criteri:

1. Rispondere allo scopo e alla severità del requisito PCI DSS originale.
2. Offrire un livello di protezione simile al requisito PCI DSS originale, ad esempio, il controllo compensativo mitiga sufficientemente il rischio per cui il requisito PCI DSS originale era stato progettato. Vedere *Navigazione in PCI DSS* per una spiegazione dello scopo di ciascun requisito PCI DSS.
3. Superare e integrare altri requisiti PCI DSS (garantire la conformità ad altri requisiti PCI DSS non è un controllo compensativo).

Per valutare un criterio di superamento dei controlli compensativi, tenere presente quanto riportato di seguito:

Nota: gli elementi descritti da a) a c) sono da intendersi semplicemente come esempi. Tutti i controlli compensativi devono essere analizzati e convalidati dal valutatore che conduce la revisione PCI DSS. L'efficacia di un controllo compensativo dipende dalle specifiche dell'ambiente in cui il controllo viene implementato, dai controlli di sicurezza circostanti e dalla configurazione del controllo. Le società devono considerare che un determinato controllo compensativo potrebbe non essere efficace in tutti gli ambienti.

- a) I requisiti PCI DSS esistenti NON POSSONO essere considerati controlli compensativi se sono già richiesti per l'elemento sottoposto a revisione. Ad esempio, le password per l'accesso amministrativo non da console devono essere inviate già cifrate per ridurre il rischio di intercettazione delle password amministrative con testo in chiaro. Un'entità non può utilizzare altri requisiti di password PCI DSS (blocco intrusioni, password complesse, ecc.) per compensare la mancanza di password cifrate, poiché tali altri requisiti di password non riducono il rischio di intercettazione delle password con testo in chiaro. Inoltre, gli altri controlli delle password rappresentano già requisiti PCI DSS per l'elemento sottoposto a revisione (password).
 - b) I requisiti PCI DSS esistenti POSSONO essere considerati controlli compensativi se sono richiesti per un'altra area, ma non sono richiesti per l'elemento sottoposto a revisione. Ad esempio, l'autenticazione a due fattori è un requisito PCI DSS per l'accesso remoto. L'autenticazione a due fattori *dalla rete interna* può anche essere considerata un controllo compensativo per l'accesso amministrativo non da console se la trasmissione di password cifrate non è supportata. L'autenticazione a due fattori può essere considerata un controllo compensativo accettabile se: (1) risponde alle intenzioni del requisito originale riducendo il rischio di intercettazione delle password amministrative con testo in chiaro e (2) è configurata correttamente e in un ambiente protetto.
 - c) I requisiti PCI DSS esistenti possono essere combinati con nuovi controlli per diventare un controllo compensativo. Ad esempio, se una società non è in grado di rendere illeggibili i dati di titolari di carta secondo il Requisito 3.4 (ad esempio, tramite cifratura), un controllo compensativo potrebbe essere composto da un dispositivo o da una combinazione di dispositivi, applicazioni e controlli che rispondano a tutte le seguenti condizioni: (1) segmentazione di rete interna; (2) filtro degli indirizzi IP o MAC; (3) autenticazione a due fattori dalla rete interna.
4. Essere adeguato al rischio ulteriore provocato dalla mancata adesione al requisito PCI DSS.

Il valutatore deve analizzare in modo approfondito i controlli compensativi durante ogni valutazione PCI DSS annuale per confermare che ogni controllo compensativo riduca adeguatamente il rischio previsto dal requisito PCI DSS originale, come definito ai punti 1-4 descritti sopra. Per mantenere la conformità,

devono essere in atto processi e controlli per garantire che i controlli compensativi rimangano attivi una volta terminata la valutazione.

Appendice C: Foglio di lavoro - Controlli compensativi

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito per il quale è stata selezionata la risposta "Sì" e sono stati specificati nella colonna "Speciale" altri controlli compensativi.

Nota: solo le società che hanno eseguito un'analisi dei rischi e presentano limitazioni aziendali tecniche o documentate legittime possono considerare l'uso dei controlli compensativi per garantire la conformità agli standard PCI DSS.

Numero e definizione del requisito:

	Informazioni richieste	Spiegazione
1. Vincoli	Elencare i vincoli che impediscono di soddisfare il requisito originale.	
2. Obiettivo	Definire l'obiettivo del controllo originale; identificare l'obiettivo soddisfatto mediante il controllo compensativo.	
3. Rischio identificato	Identificare eventuali rischi aggiuntivi dovuti alla non applicazione del controllo originale.	
4. Definizione di controlli compensativi	Definire i controlli compensativi e spiegare come soddisfano gli obiettivi del controllo originale e il rischio maggiore, se presente.	
5. Convalida dei controlli compensativi	Definire la modalità di convalida e test dei controlli compensativi.	
6. Manutenzione	Definire il processo e i controlli in atto per i controlli compensativi.	

Foglio di lavoro Controlli compensativi - Esempio

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito per il quale è stata selezionata la risposta "SI" e sono stati specificati nella colonna "Speciale" altri controlli compensativi.

Numero requisito: *8.1–Tutti gli utenti sono identificati con un nome utente univoco prima di consentire loro l'accesso a componenti del sistema o dati di titolari di carta?*

	Informazioni richieste	Spiegazione
1. Vincoli	Elencare i vincoli che impediscono di soddisfare il requisito originale.	<i>La società XYZ utilizza server Unix standalone senza LDAP. Pertanto, ciascun server richiede un login "root". Non è possibile per la società XYZ gestire il login "root" né è possibile registrare tutte le attività "root" di ciascun utente.</i>
2. Obiettivo	Definire l'obiettivo del controllo originale; identificare l'obiettivo soddisfatto mediante il controllo compensativo.	<i>L'obiettivo di richiedere login univoci è raddoppiato. In primo luogo, non è considerato accettabile da un punto di vista della sicurezza condividere credenziali di login. In secondo luogo, login condivisi rendono impossibile determinare in modo sicuro che una persona è responsabile di una determinata azione.</i>
3. Rischio identificato	Identificare eventuali rischi aggiuntivi dovuti alla non applicazione del controllo originale.	<i>La non assegnazione di ID univoci a tutti gli utenti e, di conseguenza, l'impossibilità di tenere traccia delle loro attività rappresenta un ulteriore rischio per il sistema di controllo dell'accesso.</i>
4. Definizione di controlli compensativi	Definire i controlli compensativi e spiegare come soddisfano gli obiettivi del controllo originale e il rischio maggiore, se presente.	<i>La società XYZ richiederà a tutti gli utenti di accedere ai server dai propri desktop utilizzando il comando SU. Tale comando consente a un utente di accedere all'account "root" ed eseguire le azioni come utente "root", ma essere registrato nella directory di log SU. In questo modo, le azioni di ciascun utente possono essere registrate mediante l'account SU.</i>
5. Convalida dei controlli compensativi	Definire la modalità di convalida e test dei controlli compensativi.	<i>La società XYZ dimostra al valutatore che il comando SU è in esecuzione e che gli utenti che utilizzano tale comando sono registrati per identificare l'utente che esegue le azioni con i privilegi root</i>
6. Manutenzione	Definire il processo e i controlli in atto per i controlli compensativi.	<i>La società XYZ documenta i processi e le procedure per garantire che le configurazioni SU non vengano modificate, alterate o rimosse per consentire ai singoli utenti di eseguire comandi root senza essere identificati e registrati singolarmente</i>

