



**Payment Card Industry (PCI)
Data Security Standard**

Questionario di autovalutazione B e Attestato di conformità

**Solo macchine stampigiatrici o terminali per
connessione in uscita indipendenti, nessuna
memorizzazione elettronica dei dati di titolari di
carta**

Versione 2.0

Ottobre 2010

Modifiche del documento

Data	Versione	Descrizione
1 ottobre 2008	1.2	Allineare il contenuto ai nuovi standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.
28 ottobre 2010	2.0	Allineare il contenuto ai nuovi requisiti e 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	iv
Guida per la non applicabilità di determinati requisiti specifici.....	iv
Attestato di conformità, SAQ B.....	1
Questionario di autovalutazione B	5
Protezione dei dati di titolari di carta.....	5
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati</i>	<i>5</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche.....</i>	<i>6</i>
Implementazione di rigide misure di controllo dell'accesso	7
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario... 7</i>	<i>7</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta..... 7</i>	<i>7</i>
Gestione di una politica di sicurezza delle informazioni	9
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale</i>	<i>9</i>
Appendice A: (non utilizzata).....	11
Appendice B: Controlli compensativi.....	12
Appendice C: Foglio di lavoro - Controlli compensativi.....	14
Foglio di lavoro Controlli compensativi - Esempio	15
Appendice D: Spiegazione di non applicabilità.....	16

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 B è stato sviluppato per rispondere ai requisiti applicabili ad esercenti che elaborano i dati di titolari di carta solo tramite macchinette stampigliatrici o terminali per connessione in uscita indipendenti.

La definizione degli esercenti SAQ B viene riportata qui e nel documento *Istruzioni e linee guida per il questionario di autovalutazione PCI DSS*. Gli esercenti SAQ B elaborano i dati dei titolari di carta solo tramite macchinette stampigliatrici oppure mediante terminali per connessione in uscita indipendenti e possono essere società di e-commerce con punti vendita reali (carta presente) o società di e-commerce o vendita tramite posta elettronica/telefono (carta non presente). Tali esercenti devono convalidare la propria conformità completando il questionario SAQ B e l'attestato di conformità ad esso associato, confermando che:

- La società utilizza solo macchinette stampigliatrici e/o usa solo terminali per connessione in uscita indipendenti (connessi tramite la linea telefonica al processore) per acquisire i dati della carta di pagamento dei clienti.
- I terminali per connessione in uscita indipendenti non sono connessi ad altri sistemi all'interno dell'ambiente.
- I terminali per connessione in uscita indipendenti non sono connessi a Internet.
- La società non trasmette dati dei titolari di carta di tramite una rete (rete interna o Internet).
- La società conserva solo resoconti o ricevute cartacee con i dati di titolari di carta e questi documenti non sono ricevuti in formato elettronico.
- La società non memorizza i dati di titolari di carta in formato elettronico.

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 quando 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 comunque 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 B) 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

Non applicabilità: I 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 B

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
 Market e supermarket
 Distributori di benzina
 E-Commerce
 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

In che modo e con quale titolo la società memorizza, elabora e/o trasmette dati dei titolari di carta?

Fornire le seguenti informazioni in ordine alle Applicazioni di pagamento utilizzate dalla propria azienda:

<u>Applicazione di pagamento in uso</u>	<u>Versione numero</u>	<u>Ultima convalida in base a PABP/PA-DSS</u>

Parte 2c. Idoneità al completamento del modulo SAQ B

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

<input type="checkbox"/>	L'esercente utilizza solo una macchinetta stampigliatrice per acquisire le informazioni sulla carta di pagamento dei clienti e non trasmette i dati dei titolari di carta via telefono o Internet; oppure L'esercente utilizza solo terminali di connessione remota indipendenti; tali terminali non sono connessi a Internet o ad altri sistemi disponibili nell'ambiente dell'esercente;
<input type="checkbox"/>	L'esercente non memorizza dati dei titolari di carta in formato elettronico.
<input type="checkbox"/>	L'esercente conserva i dati dei titolari di carta solo in forma di resoconti o copie di ricevute cartacee e non in formato elettronico.

Parte 3. Convalida PCI DSS

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

<input type="checkbox"/>	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 (<i>ragione sociale esercente</i>) ha dimostrato la massima conformità agli standard PCI DSS.
<input type="checkbox"/>	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 (<i>ragione sociale esercente</i>) 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. <i>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.</i>

Parte 3a. Conferma dello stato di conformità

L'esercente conferma che:

<input type="checkbox"/>	Il questionario di autovalutazione B 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.
<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> ↑
<i>Società esercente rappresentata</i> ↑	

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	
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"/>	
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 B

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:

Protezione dei dati di titolari di carta

Requisito 3: Proteggere i dati di titolari di carta memorizzati

Domanda PCI DSS		Risposta:	Sì	No	Speciale*
3.2	(b) Se sono stati ricevuti ed eliminati dati sensibili di autenticazione, sono presenti processi per l'eliminazione sicura dei dati per verificare che i dati non siano recuperabili?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Tutti i sistemi osservano i seguenti requisiti relativi alla non memorizzazione di dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati)?				
3.2.1	L'intero contenuto di ogni traccia della striscia magnetica (presente sul retro della carta, dati equivalenti contenuti in un chip o in altro luogo) non viene memorizzato in nessun caso? Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati di striscia magnetica. <i>nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</i> <ul style="list-style-type: none"> ▪ Nome del titolare della carta ▪ PAN (Primary Account Number) ▪ Data di scadenza, e ▪ Codice di servizio <i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	
3.2.3	Il numero di identificazione personale (PIN) o il blocco PIN cifrato non sono memorizzati 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>
4.2	(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"/>	

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:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
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:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
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 stati distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo che non sia possibile ricostruirli?		<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	Una politica per la sicurezza è stata definita, pubblicata, gestita e diffusa 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	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 in atto 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"/>	
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	È stato 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"/>	

Domanda PCI DSS		Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
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	È stato conservato un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi?		<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 "Sì" 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 a 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>
7. 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>
8. 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>

