



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

Questionario di autovalutazione D e Attestato di conformità

**Tutti gli altri esercenti e tutti i provider di servizi
idonei per questionario SAQ**

Versione 1.2

Ottobre 2008

Modifiche del documento

Data	Versione	Descrizione
1 ottobre 2008	1.2	Allineare il contenuto con i nuovi standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.

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 l'esclusione e la non applicabilità di determinati requisiti specifici	v
Attestato di conformità, SAQ D—Versione esercente	1
Attestato di conformità, SAQ D—Versione provider di servizi	5
Questionario di autovalutazione D	8
Sviluppo e gestione di una rete sicura.....	8
<i>Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta</i>	<i>8</i>
<i>Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di sicurezza</i>	<i>10</i>
Protezione dei dati di titolari di carta	12
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati</i>	<i>12</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche</i>	<i>15</i>
Utilizzare un programma per la gestione delle vulnerabilità	16
<i>Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus.....</i>	<i>16</i>
<i>Requisito 6: Sviluppare e gestire sistemi e applicazioni protette</i>	<i>16</i>
Implementazione di rigide misure di controllo dell'accesso	19
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario.....</i>	<i>19</i>
<i>Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer.....</i>	<i>19</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati di titolari di carta.....</i>	<i>21</i>
Monitoraggio e test delle reti regolari	24
<i>Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta.....</i>	<i>24</i>
<i>Requisito 11: Eseguire regolarmente test dei sistemi e processi di protezione</i>	<i>25</i>
Gestire una politica di sicurezza delle informazioni	27
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori</i>	<i>27</i>
Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso.....	30
<i>Requisito A.1: I provider di hosting condiviso devono proteggere l'ambiente dei dati di titolari di carta</i>	<i>30</i>
Appendice B: Controlli compensativi.....	31
Appendice C: Foglio di lavoro - Controlli compensativi.....	32
Foglio di lavoro Controlli compensativi—Esempio.....	33
Appendice D: Spiegazione di non applicabilità:.....	34

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>Requisiti PCI DSS 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 ¹
<i>PCI DSS: Questionario di autovalutazione B e Attestato</i>	Esercenti ¹
<i>PCI DSS: Questionario di autovalutazione C e Attestato</i>	Esercenti ¹
<i>PCI DSS: Questionario di autovalutazione D e Attestato</i>	Gli esercenti ¹ e tutti i provider di servizi
<i>PCI DSS e PA-DSS 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 D è stato sviluppato per tutti i provider di servizi idonei e per tutti gli esercenti che non corrispondono alle descrizioni dei questionari SAQ A-C come descritto brevemente nella tabella seguente e più dettagliatamente nel documento *Istruzioni e linee guida per l'autovalutazione PCI DSS*.

Tipo di convalida SAQ	Descrizione	SAQ
1	Esercenti con carta non presente (e-commerce o via posta/telefono), tutte le funzioni per i dati di titolari di carta sono fornite dall'esterno. <i>Non applicabile mai ad esercenti con contatto diretto con il cliente.</i>	A
2	Esercenti che utilizzano macchinetta stampigliatrice, nessuna memorizzazione elettronica dei dati di titolari di carta	B
3	Esercenti che utilizzano terminali indipendenti, nessuna memorizzazione elettronica dei dati di titolari di carta	B
4	Esercenti con sistemi POS connessi a Internet, nessuna memorizzazione elettronica dei dati di titolari di carta	C
5	Tutti gli altri esercenti (non inclusi nelle descrizioni dei questionari SAQ A-C precedenti) e tutti i provider di servizi definiti da un marchio di pagamento come idonei per completare un questionario SAQ.	D

Questi esercenti che non soddisfano i criteri dei questionari SAQ A-C sopra descritti e tutti i provider di servizi definiti da un marchio di pagamento come idonei per il questionario SAQ appartengono al Tipo di convalida SAQ 5, come definito nel presente documento e nel documento *PCI DSS: Istruzioni e linee guida per l'autovalutazione*.

Sebbene molte aziende che completano il questionario SAQ D debbano convalidare la propria conformità con ogni requisito PCI DSS, alcune aziende con modelli di business molto specifici possono trovare non applicabili alcuni requisiti. Ad esempio, una società che non utilizza una tecnologia wireless non può garantire la conformità ai requisiti indicati nelle sezioni degli standard PCI DSS specifiche di tale tecnologia. Fare riferimento alla guida seguente per informazioni sull'esclusione dei requisiti relativi alla tecnologia wireless e di determinati altri requisiti specifici.

Ciascuna sezione del questionario riguarda un'area di sicurezza specifica, in base ai requisiti degli standard di sicurezza dei dati PCI.

Conformità agli standard PCI DSS – Operazioni

1. Completare il questionario di autovalutazione (SAQ D) in *base alle istruzioni contenute nel documento Istruzioni e linee guida per l'autovalutazione*.
2. Eseguire una scansione delle vulnerabilità con esito positivo con un fornitore di scansioni approvato (ASV, Approved Scanning Vendor) da PCI SSC e ottenere un report della scansione eseguita dall'ASV.
3. Completare per intero l'attestato di conformità.
4. Inviare il questionario SAQ, il report della scansione e l'attestato di conformità, insieme ad eventuale altra documentazione richiesta, al proprio acquirente (per gli esercenti) o al marchio di pagamento o altra entità richiedente (per i provider di servizi).

Guida per l'esclusione e la non applicabilità di determinati requisiti specifici

Esclusione: Se per convalidare la propria conformità agli standard PCI DSS occorre completare il questionario SAQ D, è possibile considerare le seguenti eccezioni: 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, requisiti 1.2.3, 2.1.1, and 4.1.1). Tenere presente che occorre comunque fornire una risposta al requisito 11.1 (uso di analizzatore wireless) anche se la propria rete non prevede tecnologia wireless, perché l'analizzatore rileva eventuali intrusioni o dispositivi non autorizzati che possono essere stati aggiunti a vostra insaputa.
- Fornire una risposta alle domande specifiche di applicazioni e codice personalizzati (requisiti 6.3-6.5) solo se la propria azienda sviluppa applicazioni Web personalizzate.
- Fornire una risposta alle domande per i requisiti 9.1-9.4 solo per strutture con "aree sensibili" come definite nel presente documento. Per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.

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 per ogni voce "N/A".

Attestato di conformità, SAQ D—Versione esercente

Istruzioni per l'invio

L'esercente deve completare questo Attestato di conformità come una dichiarazione del proprio stato di conformità agli standard di sicurezza dei dati PCI. 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 su società Qualified Security Assessor (se applicabile)

Nome società:			
Nome contatto QSA principale:	Mansione:		
Telefono:	E-mail:		
Indirizzo ufficio:	Città:		
Stato/Provincia:	Paese:	CAP:	
URL:			

Parte 2. Informazioni su società esercente

Nome società:	DBA:		
Nome contatto:	Mansione:		
Telefono:	E-mail:		
Indirizzo ufficio:	Città:		
Stato/Provincia:	Paese:	CAP:	
URL:			

Parte 2a. Tipo di settore di attività dell'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 2b. Rapporti

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

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

Parte 2c. Elaborazione delle transazioni

Applicazione di pagamento in uso:	Versione applicazione di pagamento:
-----------------------------------	-------------------------------------

Parte 3. Convalida PCI DSS

In base ai risultati del questionario SAQ D datato (*completion date*), (*Merchant Company Name*) 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 e un fornitore di scansioni approvato (ASV) da PCI SSC ha eseguito una scansione di sicurezza; pertanto (*Merchant Company Name*) 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 o non è stata eseguita una scansione di sicurezza da un fornitore di scansioni approvato (ASV) da PCI SSC; pertanto (*Merchant Company Name*) 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 D PCI DSS, versione (<i>version of 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. |

² Dati codificati nella striscia magnetica 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 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 ↑

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 di 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 sicurezza	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati di titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati di 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 di titolari di carta solo se effettivamente necessario	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assegnare un ID univoco a chiunque abbia accesso a un computer	<input type="checkbox"/>	<input type="checkbox"/>	

Requisito PCI DSS	Descrizione del requisito	Stato di conformità (selezionare una risposta)		Data e azioni di correzione (in caso di non conformità)
9	Limitare l'accesso fisico ai dati di titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eseguire regolarmente test dei sistemi e processi di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni	<input type="checkbox"/>	<input type="checkbox"/>	

Attestato di conformità, SAQ D—Versione provider di servizi

Istruzioni per l'invio

Il provider di servizi deve completare questo Attestato di conformità come una dichiarazione del proprio stato di conformità agli standard di sicurezza dei dati PCI (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 su società Qualified Security Assessor (se applicabile)

Nome società:			
Nome contatto QSA principale:	Mansione:		
Telefono:	E-mail:		
Indirizzo ufficio:	Città:		
Stato/Provincia:	Paese:	CAP:	
URL:			

Parte 2. Informazioni su società provider di servizi

Nome società:			
Nome contatto:	Mansione:		
Telefono:	E-mail:		
Indirizzo ufficio:	Città:		
Stato/Provincia:	Paese:	CAP:	
URL:			

Parte 2a. Servizi

Servizi forniti (selezionare tutte le risposte appropriate):

- | | | |
|--|--|--|
| <input type="checkbox"/> Autorizzazione | <input type="checkbox"/> Programmi di fedeltà | <input type="checkbox"/> 3-D Secure Access Control Server (ACS) |
| <input type="checkbox"/> Switching | <input type="checkbox"/> IPSP (E-commerce) | <input type="checkbox"/> Elaborazione transazioni striscia magnetica |
| <input type="checkbox"/> Gateway pagamenti | <input type="checkbox"/> Compensazione e contabilizzazione | <input type="checkbox"/> Elaborazione transazioni MO/TO |
| <input type="checkbox"/> Hosting | <input type="checkbox"/> Elaborazione emissioni | <input type="checkbox"/> Altro (specificare): |

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

Parte 2b. Rapporti

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

Parte 2c: Elaborazione delle transazioni

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

Applicazioni di pagamento utilizzate o fornite nell'ambito del servizio:	Versione applicazione di pagamento:
--	-------------------------------------

Parte 3. Convalida PCI DSS

In base ai risultati del questionario SAQ D datato (*completion date of SAQ*), (*Service Provider Company Name*) 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 e un fornitore di scansioni approvato (ASV) da PCI SSC ha eseguito una scansione di sicurezza; pertanto (*Service Provider Company Name*) 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 o non è stata eseguita una scansione di sicurezza da un fornitore di scansioni approvato (ASV) da PCI SSC; pertanto (*Service Provider Company Name*) 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

Il provider di servizi conferma che:

- Il questionario di autovalutazione D, versione (*insert version number*), è stato completato in base alle istruzioni qui fornite.
- Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione.
- Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard.
- Nessuna prova di memorizzazione dei dati della striscia magnetica (traccia)⁵, CAV2, CVC2, CID, o CVV2⁶, oppure dei dati PIN⁷ dopo l'autorizzazione della transazione è stata trovata sui sistemi controllati durante questa valutazione.

Parte 3b. Accettazione da parte del provider di servizi

<i>Firma del funzionario esecutivo del provider di servizi</i> ↑	<i>Data</i> ↑
<i>Nome funzionario esecutivo del provider di servizi</i> ↑	<i>Mansione</i> ↑

Società rappresentata dal provider di servizi ↑

⁵ Dati codificati nella striscia magnetica 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.

⁶ 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.

⁷ 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 di 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 sicurezza	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati di titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati di 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 di titolari di carta solo se effettivamente necessario	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assegnare un ID univoco a chiunque abbia accesso a un computer	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati di titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eseguire regolarmente test dei sistemi e processi di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni	<input type="checkbox"/>	<input type="checkbox"/>	

Questionario di autovalutazione D

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	Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
1.1	Gli standard di configurazione del firewall e del router definiti includono quanto segue?			
1.1.1	Un processo formale per l'approvazione e il test di tutte le connessioni esterne alla rete e le modifiche apportate alla configurazione del firewall e del router?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	Diagrammi aggiornati della rete con tutte le connessioni ai dati di titolari di carta, comprese eventuali reti wireless?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	Requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Descrizione di gruppi, ruoli e responsabilità per la gestione logica dei componenti della rete?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	La documentazione e la giustificazione aziendale per l'uso di tutti i servizi, i protocolli e le porte consentite, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri?	<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	Una revisione dei set di regole del firewall e del router almeno ogni sei mesi?	<input type="checkbox"/>	<input type="checkbox"/>	
1.2	La configurazione del firewall limita 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.	Limitazione del traffico in entrata e in uscita a quello indispensabile per l'ambiente dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
1.2.2	Protezione e sincronizzazione dei file di configurazione del router?	<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Include l'installazione di firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e configura tali firewall 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"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
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?			
1.3.1	Una zona DMZ è stata implementata per limitare il traffico in entrata e in uscita ai soli protocolli necessari per l'ambiente dei dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	Il traffico Internet in entrata è stato limitato agli indirizzi IP all'interno della zona DMZ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	I percorsi diretti per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta sono stati proibiti?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	Gli indirizzi interni da Internet alla zona DMZ sono stati proibiti?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	Il traffico in uscita dall'ambiente dei dati di titolari di carta a Internet è stato limitato in modo che il traffico in uscita possa accedere solo agli indirizzi IP all'interno della zona DMZ?	<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"/>	
1.3.7	Il database è stato posizionato in una zona di rete interna, separata dalla zona DMZ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	Un IP-masquerading è stato implementato per evitare che gli indirizzi interni vengano tradotti e resi noti su Internet, tramite lo spazio indirizzi RFC 1918? <i>Utilizzare tecnologie NAT (Network Address Translation), ad esempio PAT (Port Address Translation).</i>	<input type="checkbox"/>	<input type="checkbox"/>	
1.4	Il firewall personale (software) è stato installato 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"/>	

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

Domanda		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>Ad esempio, 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	(a) I valori predefiniti** per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati sono stati modificati prima dell'installazione di un sistema wireless? <i>** Tali valori predefiniti dell'ambiente wireless includono, senza limitazione, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le impostazioni di sicurezza dei dispositivi wireless sono abilitate per l'uso della tecnologia di cifratura avanzata per l'autenticazione e la trasmissione?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Sono stati sviluppati standard di configurazione per tutti i componenti del sistema?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Questi standard affrontano tutte le vulnerabilità della sicurezza note e sono coerenti con gli standard di System Hardening che sono accettati, ad esempio, da enti quali SysAdmin Audit Network Security Network (SANS), il National Institute of Standards Technology (NIST) e il Center for Internet Security (CIS)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) I controlli assicurano quanto segue?			
2.2.1	È stata implementata una sola funzione principale per server?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	Sono stati disattivati tutti i servizi e i protocolli non necessari e non protetti (che non sono strettamente necessari per eseguire la funzione specifica di un dispositivo)?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	Sono stati configurati i parametri di protezione del sistema per prevenire eventuali usi non corretti?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	È stata rimossa tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati?	<input type="checkbox"/>	<input type="checkbox"/>	
2.3	È stata eseguita la cifratura di tutto l'accesso amministrativo non da console? <i>Utilizzare tecnologie quali SSH, VPN o SSL/TLS per la gestione basata su Web e altre attività amministrative non da console.</i>	<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		
		<u>Sì</u>	<u>No</u>	<u>Speciale*</u>
2.4	<p>In qualità di provider di hosting condiviso, i sistemi sono configurati per proteggere l'ambiente dell'entità ospitata e i dati dei titolari di carta?</p> <p>Vedere l'appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso <i>per informazioni su requisiti specifici che devono essere soddisfatti.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	

Protezione dei dati di titolari di carta

Requisito 3: *Proteggere i dati di titolari di carta memorizzati*

Domanda		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale*</u>
3.1	(a) La memorizzazione dei dati di titolari di carta è utilizzata il meno possibile e limitata, in termini di quantità di dati e tempo di memorizzazione, solo ai dati realmente necessari per fini commerciali, legali e/o legislativi?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) È in atto una politica per la conservazione e l'eliminazione dei dati, che includa le limitazioni sopra indicate (a)?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2	Tutti i sistemi aderiscono ai seguenti requisiti relativi alla memorizzazione di dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati)?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>Non memorizzare l'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, contenuto in un chip o in altro luogo). Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati di striscia magnetica.</p> <p><i>Nota: nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</i></p> <ul style="list-style-type: none"> ▪ Nome del titolare della carta ▪ PAN (Primary Account Number) ▪ Data di scadenza ▪ Codice di servizio <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari. Non memorizzare MAI il codice o valore di verifica della carta o il valore di verifica PIN.</i></p> <p><i>Nota: vedere il documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi per ulteriori informazioni.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>Non memorizzare il codice o il valore di validazione della carta (numero di tre o quattro cifre stampato sulla parte anteriore o posteriore della carta di pagamento) utilizzato per verificare le transazioni con carta non presente.</p> <p><i>Nota: vedere il documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi per ulteriori informazioni.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato.		<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale*</u>
3.3	<p>Il PAN è mascherato quando visualizzato? (Non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine)</p> <p><i>Note:</i></p> <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"/>	
3.4	<p>Il numero PAN è reso illeggibile ovunque memorizzato (inclusi i dati su supporti digitali portatili, supporti di backup e i registri) utilizzando uno dei seguenti approcci?</p> <ul style="list-style-type: none"> ▪ Hash one-way basati su crittografia avanzata ▪ Troncatura ▪ Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro) ▪ Crittografia avanzata con relativi processi e procedure di gestione delle chiavi. <p><i>Il PAN è l'informazione MINIMA sull'account che deve essere resa illeggibile.</i></p> <p><i>In caso di problemi nel rendere illeggibile il numero PAN, consultare l'Appendice B: "Controlli compensativi".</i></p> <p><i>Nota: La "crittografia avanzata" viene definita nel documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	<p>Se si utilizza la cifratura su disco (anziché la cifratura del database a livello di file o colonna):</p>				
	(a) L'accesso logico è gestito in modo indipendente dai meccanismi nativi di controllo dell'accesso al sistema operativo (ad esempio, evitando di utilizzare i database di account utente locali)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le chiavi di decifratura sono indipendenti dagli account utente?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	Le chiavi utilizzate per la crittografia di dati di titolari di carta sono protette da divulgazione e uso improprio?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.1	L'accesso alle chiavi utilizzate per la crittografia è limitato al minor numero possibile di persone necessarie?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	Le chiavi utilizzate per la crittografia sono custodite in un luogo sicuro e nel minor numero possibile di luoghi e formati?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6	<p>(a) Tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta sono completamente documentati e implementati?</p> <p>(b) Includono quanto segue?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.1	Generazione di chiavi di crittografia avanzata		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Distribuzione sicura delle chiavi di crittografia		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda		Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
3.6.3	Memorizzazione sicura delle chiavi di crittografia	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Modifica periodica delle chiavi di crittografia <ul style="list-style-type: none"> ▪ In base a quanto richiesto e consigliato dall'applicazione associata (ad esempio, re-keying), preferibilmente in modo automatico ▪ Almeno una volta all'anno 	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Ritiro o sostituzione di chiavi di crittografia precedentemente o potenzialmente compromesse	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Uso della procedura "split knowledge" e definizione del controllo duale delle chiavi di crittografia	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Obbligo per i custodi delle chiavi di crittografia di firmare una dichiarazione in cui accettano e confermano di conoscere le proprie responsabilità.	<input type="checkbox"/>	<input type="checkbox"/>	

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

Domanda		Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
4.1	<p>I protocolli di crittografia e sicurezza avanzati, quali SSL/TLS o IPSEC, sono stati utilizzati per proteggere i dati sensibili di titolari di carta durante la trasmissione su reti pubbliche e aperte?</p> <p><i>Esempi di reti pubbliche aperte che rientrano nell'ambito degli standard PCI DSS sono la rete Internet, le tecnologie wireless, le reti GSM (Global System for Mobile communications) e le reti GPRS (General Packet Radio Service).</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	<p>Le pratiche di settore consigliate (ad esempio, IEEE 802.11i) sono state utilizzate per implementare la cifratura avanzata per l'autenticazione e la trasmissione per le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta?</p> <p><i>Note:</i></p> <ul style="list-style-type: none"> ▪ <i>Per le nuove implementazioni wireless, non è consentito implementare la tecnologia WEP dopo il 31 marzo 2009.</i> ▪ <i>Per le implementazioni wireless correnti, non è consentito utilizzare la tecnologia WEP dopo il 30 giugno 2010.</i> 	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	<p>Sono in atto politiche, procedure e azioni per precludere l'invio di PAN non cifrati mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, chat)?</p>	<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Utilizzare un programma per la gestione delle vulnerabilità

Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus

Domanda	Risposta:	Risposta:		Speciale*
		Si	No	
5.1	È stato installato un programma antivirus su tutti i sistemi, in particolare PC e server, comunemente colpiti da malware?	<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Tutti i programmi antivirus sono in grado di rilevare e rimuovere tutti i tipi di malware noti?	<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Tutti i meccanismi antivirus sono aggiornati, in esecuzione e in grado di generare log di audit?	<input type="checkbox"/>	<input type="checkbox"/>	

Requisito 6: Sviluppare e gestire sistemi e applicazioni protette

Domanda	Risposta:	Risposta:		Speciale*
		Si	No	
6.1	(a) Sono state installate le ultime patch di protezione disponibili su tutti i componenti del sistema e i programmi software in uso?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono state installate patch di protezione critiche entro un mese dal relativo rilascio? <i>Nota: è possibile adottare un approccio basato su rischio per dare priorità alle installazioni delle patch. Ad esempio, dare la massima priorità all'infrastruttura critica (dispositivi e sistemi rivolti al pubblico e database), rispetto ai dispositivi interni meno importanti, per garantire che le patch necessarie vengano installate sui sistemi e sui dispositivi ad alta priorità entro un mese e su altri dispositivi e sistemi meno importanti entro tre mesi.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) È in atto un processo per identificare vulnerabilità della sicurezza recentemente rilevate (ad esempio, attraverso un abbonamento a servizi di notifica gratuiti disponibili in Internet)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Gli standard di configurazione sono stati aggiornati secondo il Requisito 2.2 PCI DSS per risolvere nuovi problemi di vulnerabilità?	<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Le applicazioni software sono state sviluppate in base agli standard PCI DSS (ad esempio, autenticazione e registrazione sicure) e alle pratiche di settore consigliate, quindi incorporano la protezione delle informazioni nell'intero ciclo di sviluppo del software?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I controlli assicurano quanto segue?			
6.3.1	Tutte le patch di sicurezza e le modifiche di configurazione del sistema e del software vengono sottoposte a test prima di essere distribuite, incluso, senza limitazione, quanto segue:	<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
6.3.1.1	Convalida di tutto l'input (per prevenire cross-site scripting, injection flaw, esecuzione di file pericolosi, ecc.)	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.1.2	Convalida del processo di gestione degli errori appropriato	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.1.3	Convalida del processo di memorizzazione di dati crittografici sicuro	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.1.4	Convalida di comunicazioni sicure	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.1.5	Convalida di un processo di controllo dell'accesso basato su ruoli (RBAC, Role-Based Access Control) appropriato	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.2	Gli ambienti di sviluppo/test e produzione sono separati?	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.3	Le responsabilità assegnate agli ambienti di sviluppo/test e produzione sono separate?	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.4	I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo?	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.5	Dati e account di test vengono rimossi prima dell'attivazione dei sistemi di produzione?	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.6	Account, ID utente e password di applicazioni personalizzate vengono rimossi prima dell'attivazione o della distribuzione di tali applicazioni ai clienti?	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.7	Il codice personalizzato viene analizzato prima del rilascio in produzione o della distribuzione ai clienti per identificare eventuali vulnerabilità? <i>Nota: questo requisito per le analisi del codice si applica a tutti i codici personalizzati (interni ed esterni), come parte della durata del ciclo di sviluppo del sistema richiesto nel Requisito 6.3 PCI DSS. Le analisi del codice possono essere condotte da personale interno preparato. Le applicazioni Web sono anche soggette a controlli aggiuntivi, se sono pubbliche, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.</i>	<input type="checkbox"/>	<input type="checkbox"/>			
6.4	(a) Le procedure di controllo delle modifiche sono state seguite per tutte le modifiche da apportare ai componenti di sistema?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Le procedure assicurano quanto segue?					
6.4.1	Documentazione dell'impatto?	<input type="checkbox"/>	<input type="checkbox"/>			
6.4.2	Approvazione del management delle parti interessate?	<input type="checkbox"/>	<input type="checkbox"/>			
6.4.3	Test della funzionalità operativa?	<input type="checkbox"/>	<input type="checkbox"/>			
6.4.4	Procedure di back-out?	<input type="checkbox"/>	<input type="checkbox"/>			
6.5	(a) Tutte le applicazioni Web (interne, esterne e con accesso amministrativo all'applicazione tramite Web) sono state sviluppate in base alle linee guida di codifica sicura, quali <i>Open Web Application Security Project Guide</i> ?	<input type="checkbox"/>	<input type="checkbox"/>			

Domanda		Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
(b) I processi di sviluppo del software prevengono eventuali vulnerabilità del codice, incluso quanto segue? <i>Nota: Le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nella guida OWASP al momento della pubblicazione degli standard PCI DSS v1.2. Tuttavia, in caso di aggiornamento della guida OWASP, è necessario utilizzare la versione più recente per questi requisiti.</i>				
6.5.1	XSS (Cross-Site Scripting)?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Injection flaw, in particolare SQL injection? <i>Considerare, inoltre, LDAP e Xpath injection flaw, nonché altri tipi di injection flaw.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Esecuzione di file pericolosi?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Riferimenti a oggetti diretti non sicuri?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Cross-site request forgery (CSRF)?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	Perdita di informazioni e gestione degli errori non appropriata?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.7	Violazione dell'autenticazione e gestione delle sessioni?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Memorizzazione di dati crittografici non sicura?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Comunicazioni non sicure?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.10	Errore di limitazione dell'accesso URL?	<input type="checkbox"/>	<input type="checkbox"/>	
6.6	Per le applicazioni Web esterne, la protezione da nuove minacce e vulnerabilità è assicurata costantemente, e queste applicazioni sono protette da attacchi noti mediante uno dei seguenti metodi? <ul style="list-style-type: none"> ▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi di valutazione della sicurezza delle applicazioni manuali o automatici, almeno una volta all'anno e dopo ogni modifica. ▪ Installazione di un firewall a livello di applicazioni Web davanti alle applicazioni Web rivolte al pubblico. 	<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		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale*</u>
7.1	(a) 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?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le limitazioni di accesso devono includere quanto segue:				
7.1.1	Limitazione dei diritti di accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Richiesta di un modulo di autorizzazione firmato dal management che specifica i privilegi necessari?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Implementazione di un sistema di controllo dell'accesso automatico?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	(a) Per sistemi con più utenti, è adottato un meccanismo di controllo dell'accesso in base alla reale necessità di un utente ed è impostato su "deny all" per impedire ogni accesso se non specificatamente consentito?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il sistema di controllo dell'accesso deve includere quanto segue:				
7.2.1	Copertura di tutti i componenti di sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Impostazione predefinita "deny all"?		<input type="checkbox"/>	<input type="checkbox"/>	

Requisito 8: *Assegnare un ID univoco a chiunque abbia accesso a un computer*

Domanda		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale*</u>
8.1	A tutti gli utenti viene assegnato un ID univoco prima di consentire loro l'accesso a componenti del sistema o dati di titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	
8.2	Oltre ad assegnare un ID univoco, viene adottato uno o più dei seguenti metodi per autenticare tutti gli utenti? <ul style="list-style-type: none"> ▪ Password o passphrase ▪ Autenticazione a due fattori (ad esempio, dispositivi token, smart card, biometrica o chiavi pubbliche) 		<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
8.3	L'autenticazione a due fattori è incorporata per l'accesso remoto alla rete (accesso a livello di rete dall'esterno) da parte di dipendenti, amministratori e terze parti? <i>Utilizzare tecnologie, quali RADIUS (Remote Authentication and Dial-In Service) o TACACS (Terminal Access Controller Access Control System) con token oppure VPN (basata su SSL/TLS o IPSEC) con certificati individuali.</i>	<input type="checkbox"/>	<input type="checkbox"/>			
8.4	Tutte le password sono rese illeggibili durante la trasmissione e la memorizzazione su tutti i componenti di sistema tramite la crittografia avanzata (definita nel documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>)?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5	Sono in atto controlli della gestione delle autenticazioni e delle password utente per utenti non consumatori e amministratori in tutti i componenti del sistema, nel seguente modo?					
8.5.1	Le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi sono controllate?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.2	L'identità dell'utente viene verificata prima del ripristino della password?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.3	Le password per il primo accesso sono impostate su un valore univoco per ciascun utente? Ogni utente modifica la propria password immediatamente dopo il primo accesso?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.4	L'accesso per gli utenti non attivi viene revocato immediatamente?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.5	Gli account utente non attivi vengono rimossi o disattivati almeno ogni 90 giorni?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.6	Gli account utilizzati dai fornitori per la gestione in remoto sono abilitati solo durante il periodo di tempo necessario?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.7	Le procedure e le politiche relative alle password vengono comunicate a tutti gli utenti con accesso ai dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.8	Gli account e le password di gruppo, condivisi o generici sono stati proibiti?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.9	Le password utente devono essere modificate almeno ogni 90 giorni?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.10	La lunghezza minima della password è impostata su 7 caratteri?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.11	Le password devono contenere caratteri numerici e alfabetici?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.12	La nuova password specificata deve essere diversa dalle ultime quattro password utilizzate?	<input type="checkbox"/>	<input type="checkbox"/>			
8.5.13	I tentativi di accesso ripetuti sono limitati bloccando l'ID utente dopo un massimo di sei tentativi?	<input type="checkbox"/>	<input type="checkbox"/>			

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		
		Si	No	Speciale*
8.5.14	La durata del blocco è impostata su un minimo di 30 minuti o fino a quando l'amministratore non abilita nuovamente l'ID utente?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	Se una sessione è inattiva per più di 15 minuti, l'utente deve immettere nuovamente la password per riattivare il terminale?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	Tutti gli accessi al database contenente i dati di titolari di carta sono autenticati? (Sono compresi gli accessi da applicazioni, amministratori e tutti gli altri utenti).	<input type="checkbox"/>	<input type="checkbox"/>	

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

Domanda		Risposta:		
		Si	No	Speciale*
9.1	I controlli dell'accesso alle strutture appropriati sono utilizzati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) Le videocamere o altri meccanismi di controllo dell'accesso sono utilizzati per monitorare gli accessi fisici ad aree sensibili? <i>Nota: per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I dati raccolti dalle videocamere sono controllati e correlati con altri dati?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) I dati delle videocamere sono conservati per almeno tre mesi, se non diversamente specificato dalla legge?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.2	L'accesso fisico a connettori di rete accessibili pubblicamente è limitato?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	L'accesso fisico a punti di accesso wireless, gateway e dispositivi portatili è limitato?	<input type="checkbox"/>	<input type="checkbox"/>	
9.2	Sono in atto procedure che consentono al tutto il personale di distinguere facilmente tra dipendenti e visitatori, in particolare in aree che permettono l'accesso ai dati di titolari di carta? <i>Ai fini del presente requisito, per "dipendente" 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. Per "visitatore" si intende un fornitore, un ospite di un dipendente, un tecnico dell'assistenza o chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente non più di un giorno.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
9.3	Tutti i visitatori sono gestiti nel seguente modo:			

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
9.3.1	Ricevono l'autorizzazione appropriata prima di accedere alle aree in cui i dati di titolari di carta sono elaborati o custoditi?	<input type="checkbox"/>	<input type="checkbox"/>			
9.3.2	Ricevono un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) che scade e che identifica i visitatori come non dipendenti?	<input type="checkbox"/>	<input type="checkbox"/>			
9.3.3	Restituiscono il token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza?	<input type="checkbox"/>	<input type="checkbox"/>			
9.4	(a) È in uso un registro dei visitatori per mantenere un audit trail fisico dell'attività dei visitatori?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Il nome del visitatore, l'azienda rappresentata e il dipendente che autorizza l'accesso fisico sono documentati sul registro?	<input type="checkbox"/>	<input type="checkbox"/>			
	(c) Viene conservato un registro dei visitatori per almeno tre mesi, se non diversamente richiesto dalla legge?	<input type="checkbox"/>	<input type="checkbox"/>			
9.5	(a) I backup dei supporti sono conservati in un luogo sicuro, preferibilmente in una struttura esterna, quale un luogo alternativo o di backup oppure un magazzino?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) La sicurezza del luogo viene controllata almeno una volta all'anno?	<input type="checkbox"/>	<input type="checkbox"/>			
9.6	Tutti i supporti cartacei ed elettronici contenenti i dati dei titolari di carta sono conservati in un luogo fisicamente sicuro?	<input type="checkbox"/>	<input type="checkbox"/>			
9.7	(a) La distribuzione interna ed esterna di qualsiasi tipo di supporto contenente dati di titolari di carta 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 che possa essere identificato come contenente dati riservati?	<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 monitorato in modo appropriato?	<input type="checkbox"/>	<input type="checkbox"/>			
9.8	Sono in atto processi e procedure per garantire che il management abbia dato l'approvazione prima di spostare qualsiasi supporto contenente dati di titolari da un'area protetta (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 a supporti contenenti dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>			
9.9.1	(a) I registri di inventario per tutti i supporti sono stati conservati in modo appropriato?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Gli inventari dei supporti vengono eseguiti almeno una volta l'anno?	<input type="checkbox"/>	<input type="checkbox"/>			
9.10	I supporti contenenti dati di titolari di carta vengono distrutti quando non sono più necessari per scopi aziendali o legali? I supporti devono essere eliminati in uno dei seguenti modi:	<input type="checkbox"/>	<input type="checkbox"/>			

Domanda		Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
9.10.1	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"/>	
9.10.2	I dati dei titolari di carta su supporti elettronici sono resi non recuperabili, in modo che non sia possibile ricostruirli?	<input type="checkbox"/>	<input type="checkbox"/>	

Monitoraggio e test delle reti regolari

Requisito 10: *Registrazione e monitoraggio di tutti gli accessi a risorse di rete e dati di titolari di carta*

Domanda		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale*</u>
10.1	È in atto un processo per collegare tutto l'accesso ai componenti del sistema (in particolare l'accesso eseguito con privilegi di amministratore, ad esempio come utente root) a ciascun utente?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2	Sono stati implementati audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:				
10.2.1	Tutti i singoli accessi di utenti a dati di titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.2	Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.3	Accesso a tutti gli audit trail?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Tentativi di accesso logico non validi?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Uso di meccanismi di identificazione e autenticazione?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.6	Inizializzazione di log di audit?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.7	Creazione ed eliminazione di oggetti a livello di sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3	Vengono registrate le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:				
10.3.1	Identificazione utente?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Tipo di evento?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Data e ora?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Indicazione di successo o fallimento?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Origine dell'evento?		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa)?		<input type="checkbox"/>	<input type="checkbox"/>	
10.4	Tutti gli orologi e gli orari critici del sistema sono sincronizzati?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) Gli audit trail sono protetti in modo che non possano essere modificati?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I controlli assicurano quanto segue?				
10.5.1	La visualizzazione degli audit trail è limitata a coloro che realmente necessitano di tali informazioni per scopi aziendali?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.2	I file di audit trail sono protetti da modifiche non autorizzate?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.3	Viene eseguito il backup dei file di audit trail su un server dei log o un supporto centralizzato difficile da modificare?		<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:	Si	No	Speciale*
10.5.4	I registri per le tecnologie rivolte al pubblico vengono create su un server di log sulla LAN interna?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	Vengono utilizzati un meccanismo di monitoraggio dell'integrità dei file o un software di rilevamento delle modifiche di log per accertarsi che i dati di log esistenti non possano essere modificati senza generare avvisi (non per l'aggiunta di nuovi dati)?		<input type="checkbox"/>	<input type="checkbox"/>	
10.6	I log per tutti i componenti di sistema vengono esaminati almeno una volta al giorno? <i>Le analisi dei log devono includere i server che eseguono funzioni di sicurezza, quali i servizi antintrusione IDS (Intrusion Detection System), i server di autenticazione, autorizzazione e accounting (AAA), ad esempio RADIUS.</i> <i>Nota: gli strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità al requisito 10.6.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	La cronologia dell'audit trail è stata conservata per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup)?		<input type="checkbox"/>	<input type="checkbox"/>	

Requisito 11: Eseguire regolarmente test dei sistemi e processi di protezione

Domanda		Risposta:	Si	No	Speciale*
11.1	La presenza di punti di accesso wireless è stata verificata utilizzando un analizzatore wireless almeno una volta ogni tre mesi oppure distribuendo un IDS/IPS wireless per identificare tutti i dispositivi wireless in uso?		<input type="checkbox"/>	<input type="checkbox"/>	
11.2	Sono state eseguite scansioni interne ed esterne della rete almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, l'installazione di nuovi componenti di sistema, la modifica della topologia della rete, la modifica delle regole del firewall o l'aggiornamento di un prodotto)? <i>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di scansioni approvato (ASV) e qualificato da PCI SSC. Le scansioni dopo le modifiche della rete possono essere eseguite dal personale interno della società.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
11.3	(a) I test di penetrazione esterna ed interna vengono eseguiti almeno una volta l'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I test di penetrazione includono quanto segue:				
11.3.1	Test di penetrazione a livello di rete?		<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Test di penetrazione a livello di applicazione?		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda		Risposta:		
		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
11.4	(a) Vengono utilizzati sistemi di rilevamento e/o di prevenzione delle intrusioni per monitorare tutto il traffico nell'ambiente dei dati di titolari di carta e segnalare possibili rischi al personale addetto?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Tutti i moduli di rilevamento e prevenzione delle intrusioni sono mantenuti aggiornati?	<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) Viene distribuito al personale addetto un software di monitoraggio dell'integrità dei file per segnalare eventuali modifiche non autorizzate di file di sistema, di configurazione o di contenuto critici?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il software è configurato per eseguire confronti di file critici almeno una volta a settimana? <i>Nota: ai fini del monitoraggio dell'integrità dei file, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. In genere, i prodotti per il monitoraggio dell'integrità dei file sono preconfigurati con file critici per il sistema operativo in uso. Altri file critici, ad esempio quelli per applicazioni personalizzate, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).</i>	<input type="checkbox"/>	<input type="checkbox"/>	

Gestire una politica di sicurezza delle informazioni

Requisito 12: *Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori*

Domanda		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
12.1	È stata definita, pubblicata, gestita e diffusa una politica per la sicurezza che prevede quanto segue:	<input type="checkbox"/>	<input type="checkbox"/>			
12.1.1	Risponde a tutti i requisiti PCI DSS?	<input type="checkbox"/>	<input type="checkbox"/>			
12.1.2	Include un processo annuale per identificare minacce e vulnerabilità, che consente di ottenere una valutazione dei rischi formale?	<input type="checkbox"/>	<input type="checkbox"/>			
12.1.3	Include una revisione almeno una volta l'anno e aggiornamenti in caso di cambiamenti dell'ambiente?	<input type="checkbox"/>	<input type="checkbox"/>			
12.2	Sono state sviluppate procedure di sicurezza operativa giornaliere coerenti con i requisiti di questa specifica (ad esempio, procedure per la manutenzione degli account utente e procedure di analisi dei log)?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3	(a) Le politiche di uso per tecnologie per dipendenti critiche (ad esempio, tecnologie di accesso remoto, wireless, supporti elettronici rimovibili, laptop, PDA, uso della posta elettronica e di Internet) sono sviluppate per definire l'uso corretto di queste tecnologie per tutti i dipendenti e i collaboratori esterni. (b) Queste politiche richiedono quanto segue?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.1	Approvazione esplicita del management?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.2	Autenticazione per l'uso della tecnologia?	<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"/>			
12.3.4	Etichettatura di dispositivi con proprietario, informazioni di contatto e scopo?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.5	Usi accettabili delle tecnologie?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.6	Posizioni di rete accettabili per le tecnologie?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.7	Elenco di prodotti approvati dalla società?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.8	Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività?	<input type="checkbox"/>	<input type="checkbox"/>			
12.3.9	Attivazione di tecnologie di accesso remoto per i fornitori solo quando richiesto dai fornitori, con disattivazione immediata dopo l'uso?	<input type="checkbox"/>	<input type="checkbox"/>			

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
12.3.10	Durante l'accesso ai dati di titolari di carta tramite tecnologie di accesso remoto, la politica specifica la proibizione di copia, spostamento e memorizzazione dei dati di titolari di carta su dischi rigidi locali e supporti elettronici rimovibili?	<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 tutti i dipendenti e i collaboratori?	<input type="checkbox"/>	<input type="checkbox"/>			
12.5	Sono state assegnate le seguenti responsabilità per la gestione della sicurezza delle informazioni a una singola persona o a un team?					
12.5.1	Definizione, documentazione e distribuzione delle politiche e delle procedure di sicurezza?	<input type="checkbox"/>	<input type="checkbox"/>			
12.5.2	Monitoraggio e analisi degli avvisi e delle informazioni sulla sicurezza e distribuzione al personale appropriato?	<input type="checkbox"/>	<input type="checkbox"/>			
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"/>			
12.5.4	Amministrazione di account utente, incluse aggiunte, eliminazione e modifiche?	<input type="checkbox"/>	<input type="checkbox"/>			
12.5.5	Monitoraggio e controllo di tutti gli accessi ai dati?	<input type="checkbox"/>	<input type="checkbox"/>			
12.6	È in atto un programma formale di consapevolezza della sicurezza per rendere tutti i dipendenti consapevoli dell'importanza della sicurezza dei dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>			
12.6.1	I dipendenti vengono formati al momento dell'assunzione e almeno una volta all'anno?	<input type="checkbox"/>	<input type="checkbox"/>			
12.6.2	Viene richiesto ai dipendenti di firmare almeno una volta l'anno un documento che attesti che hanno letto e compreso la politica e le procedure di sicurezza della società?	<input type="checkbox"/>	<input type="checkbox"/>			
12.7	I potenziali dipendenti sono sottoposti a screening (vedere la definizione di "dipendente" al punto 9.2 riportato sopra) prima di essere assunti per ridurre al minimo il rischio di attacchi da fonti interne? <i>Per i dipendenti, quali i cassieri di un negozio, che hanno accesso a un solo numero di carta alla volta, questo requisito è solo consigliato.</i>	<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 sono gestite e implementate per la gestione dei provider di servizi, e le politiche e le procedure includono quanto segue?	<input type="checkbox"/>	<input type="checkbox"/>			
12.8.1	È stato conservato un elenco di provider di servizi.	<input type="checkbox"/>	<input type="checkbox"/>			

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

Domanda		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale*</u>
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"/>			
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"/>			
12.9	È stato implementato un piano di risposta che includa quanto segue in preparazione alla risposta immediata a una violazione del sistema?					
12.9.1	(a) È stato creato un piano di risposta da implementare nel caso di violazione del sistema?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Il piano deve includere almeno i seguenti elementi:					
	▪ Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento	<input type="checkbox"/>	<input type="checkbox"/>			
	▪ Procedure specifiche di risposta agli incidenti	<input type="checkbox"/>	<input type="checkbox"/>			
	▪ Procedure di ripristino e continuità delle attività aziendali	<input type="checkbox"/>	<input type="checkbox"/>			
	▪ Processi di backup dei dati	<input type="checkbox"/>	<input type="checkbox"/>			
	▪ Analisi dei requisiti legali per la segnalazione delle violazioni	<input type="checkbox"/>	<input type="checkbox"/>			
	▪ Copertura e risposte per tutti i componenti di sistema critici	<input type="checkbox"/>	<input type="checkbox"/>			
	▪ Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento	<input type="checkbox"/>	<input type="checkbox"/>			
12.9.2	Il piano viene sottoposto a test almeno una volta l'anno?	<input type="checkbox"/>	<input type="checkbox"/>			
12.9.3	Per rispondere a eventuali problemi è disponibile personale specifico 24 ore su 24, 7 giorni alla settimana?	<input type="checkbox"/>	<input type="checkbox"/>			
12.9.4	Viene fornita la formazione appropriata al personale con responsabilità di risposta a violazioni della sicurezza?	<input type="checkbox"/>	<input type="checkbox"/>			
12.9.5	Vengono inclusi avvisi dei sistemi di rilevamento delle intrusioni, prevenzione delle intrusioni e monitoraggio dell'integrità dei file?	<input type="checkbox"/>	<input type="checkbox"/>			
12.9.6	È stato sviluppato e messo in atto un processo per la modifica e il miglioramento del piano di risposta agli incidenti in base a quanto appreso e per incorporare gli sviluppi del settore?	<input type="checkbox"/>	<input type="checkbox"/>			

Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso

Requisito A.1: I provider di hosting condiviso devono proteggere l'ambiente dei dati di titolari di carta

Domanda	Risposta:			
	<u>Si</u>	<u>No</u>	<u>Speciale*</u>	
<p>A.1 L'ambiente e i dati di ciascuna entità ospitata (esercente, provider di servizi o altra entità) sono protetti nei modi previsti dal punto A.1.1 al punto A.1.4:</p> <p><i>Il provider di hosting è tenuto a soddisfare questi requisiti, oltre a tutte le altre sezioni rilevanti degli standard PCI DSS.</i></p> <p><i>Nota: anche se un provider di hosting soddisfa tutti questi requisiti, la conformità dell'entità che utilizza tale provider di hosting non è automaticamente garantita. Ogni entità deve soddisfare i requisiti e ottenere la convalida della conformità agli standard PCI DSS, come applicabile.</i></p>				
A.1.1	Ogni entità esegue processi con accesso esclusivo al proprio ambiente dei dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	L'accesso e i privilegi di ciascuna entità sono limitati al relativo ambiente di dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	Le funzioni di generazione di log e audit trail sono abilitate e specifiche per l'ambiente di dati di titolari di carta di ciascuna entità e coerenti al requisito 10 degli standard PCI DSS?	<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	Sono abilitati processi per fornire tutte le informazioni necessarie per un'indagine legale tempestiva in caso di violazione di dati di un esercente o un provider di servizi ospitato?	<input type="checkbox"/>	<input type="checkbox"/>	

* "Non Applicabile" (N/A) o "Controllo compensativo utilizzato". Le aziende che utilizzano questa sezione devono completare l'apposito foglio di lavoro "Controllo compensativo" o "Spiegazione di non applicabilità" nell'appendice.

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 "SI" 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>
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>

