



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

Questionario di autovalutazione D e Attestato di conformità

**Tutti gli altri esercenti e provider di servizi idonei
al questionario SAQ**

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.....	vi
Attestato di conformità, SAQ D – Versione esercente	1
Attestato di conformità, SAQ D–Versione provider di servizi	1
Questionario di autovalutazione D	1
Sviluppo e gestione di una rete sicura.....	1
<i>Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta.....</i>	<i>1</i>
<i>Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione</i>	<i>4</i>
Protezione dei dati di titolari di carta.....	7
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati</i>	<i>7</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche</i>	<i>11</i>
Utilizzare un programma per la gestione delle vulnerabilità.....	12
<i>Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus.....</i>	<i>12</i>
<i>Requisito 6: Sviluppare e gestire sistemi e applicazioni protette</i>	<i>12</i>
Implementazione di rigide misure di controllo dell'accesso	17
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario..</i>	<i>17</i>
<i>Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer.....</i>	<i>18</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati dei 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>26</i>
Gestione di una politica di sicurezza delle informazioni	30
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale.....</i>	<i>30</i>
Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso	34
<i>Requisito A.1: I provider di hosting condiviso devono proteggere l'ambiente dei dati di titolari di carta.....</i>	<i>34</i>
Appendice B: Controlli compensativi.....	36
Appendice C: Foglio di lavoro - Controlli compensativi.....	38
Foglio di lavoro Controlli compensativi - Esempio	39
Appendice D: Spiegazione di non applicabilità.....	40

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 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*.

SAQ	Descrizione
A	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>
B	Esercenti che utilizzano solo macchinetta stampigliatrice senza alcuna memorizzazione elettronica dei dati di titolari di carta, oppure esercenti con terminali per connessione in uscita indipendenti senza alcuna memorizzazione elettronica dei dati di titolari di carta
C-VT	Esercenti che utilizzano solo terminali virtuali basati su Web, senza alcuna memorizzazione elettronica dei dati di titolari di carta
C	Esercenti con sistemi di pagamento connessi a Internet, nessuna memorizzazione dei dati di titolari di carta
D	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.

Il questionario SAQ D riguarda gli esercenti idonei per il questionario SAQ che non soddisfano i criteri per i questionari SAQ A-C precedenti e tutti i provider di servizi definiti da un marchio di pagamento come idonei alla compilazione del questionario SAQ. Gli esercenti ed i provider di servizi SAQ D convalidano la propria conformità completando il questionario SAQ D e l'attestato di conformità ad esso associato. 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 in alcun modo non può garantire la conformità ai requisiti indicati nelle sezioni degli standard PCI DSS specifiche per la gestione 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 negli 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 D) in base alle istruzioni contenute nel documento *Istruzioni e linee guida per l'autovalutazione*.
3. 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.
4. Completare per intero l'attestato di conformità.

5. 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 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 e 4.1.1). Tenere presente che occorre comunque fornire una risposta al requisito 11.1 (uso di un processo per identificare punti di accesso wireless non autorizzati) anche se la propria rete non prevede la tecnologia wireless, perché il processo 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 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 intendono 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 sono presenti solo terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio, ma comprende le sale server back-office di negozi di vendita al dettaglio in cui sono memorizzati dati dei titolari di carta e aree di memorizzazione per grandi quantità di tali dati.

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

Attestato di conformità, SAQ 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 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 settore di attività dell'esercente (selezionare tutte le risposte applicabili):

- Rivenditore Telecomunicazioni Negozi di alimentari e supermercati
 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, eccetera)? 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 3. Convalida PCI DSS

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

Conforme: Tutte le sezioni del questionario SAQ PCI sono state completate e a tutte le domande è stato risposto affermativamente, determinando una valutazione di **CONFORMITÀ** globale e un fornitore di scansioni approvato (ASV) da PCI SSC ha eseguito una scansione di sicurezza; pertanto (*ragione sociale esercente*) ha dimostrato la massima conformità agli standard PCI DSS.

Non conforme: Non tutte le sezioni del questionario SAQ PCI sono state completate e ad alcune domande è stato risposto "no", determinando una valutazione di **NON CONFORMITÀ** globale o non è stata eseguita una scansione di sicurezza da un fornitore di scansioni approvato (ASV) da PCI SSC; pertanto (*ragione sociale esercente*) non ha dimostrato la massima conformità agli standard PCI DSS.

Data di scadenza per conformità:

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

Parte 3a. Conferma dello stato di conformità

L'esercente conferma che:

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

Parte 3b. Accettazione da parte dell'esercente

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.

<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> ↑	

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

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

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

		Stato di conformità (selezionare una risposta)		
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eeguire regolarmente test dei sistemi e processi di protezione	<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"/>	

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 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 ed azienda qualificata per la valutazione (QSA)

Parte 1a. Informazioni su società provider di servizi

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. Informazioni valutazione PCI DSS

Parte 2a. Servizi forniti che ERANO COMPRESI nell'ambito della valutazione PCI DSS (selezionare tutte le risposte applicabili)

<input type="checkbox"/> Provider di hosting sicuro 3-D	<input type="checkbox"/> Provider di hosting – Hardware	<input type="checkbox"/> Elaborazione pagamento – ATM
<input type="checkbox"/> Gestione account	<input type="checkbox"/> Provider di hosting – Web	<input type="checkbox"/> Elaborazione pagamento – MOTO
<input type="checkbox"/> Autorizzazione	<input type="checkbox"/> Elaborazione emittente	<input type="checkbox"/> Elaborazione pagamento – Internet
<input type="checkbox"/> Servizi di back-office	<input type="checkbox"/> Programmi di fedeltà	<input type="checkbox"/> Elaborazione pagamento – POS
<input type="checkbox"/> Gestione fatturazione	<input type="checkbox"/> Servizi gestiti	<input type="checkbox"/> Servizi prepagati
<input type="checkbox"/> Compensazione contabilizzazione e	<input type="checkbox"/> Servizi esercenti	<input type="checkbox"/> Gestione registrazioni
<input type="checkbox"/> Preparazione dati	<input type="checkbox"/> Provider di rete/Trasmettitore	<input type="checkbox"/> Pagamenti pubblici/fiscali
<input type="checkbox"/> Servizi di storno di addebito e frode	<input type="checkbox"/> Gateway/Switch di pagamento	
<input type="checkbox"/> Altro (specificare):		

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

Parte 2b. Se il provider di servizi fornisce i servizi elencati ma gli stessi *NON SONO STATI INSERITI* nell'ambito della valutazione PCI DSS Assessment, selezionarli di seguito:

<input type="checkbox"/> Provider di hosting sicuro 3-D	<input type="checkbox"/> Provider di hosting – Hardware	<input type="checkbox"/> Elaborazione pagamento – ATM
<input type="checkbox"/> Gestione account	<input type="checkbox"/> Provider di hosting – Web	<input type="checkbox"/> Elaborazione pagamento – MOTO
<input type="checkbox"/> Autorizzazione	<input type="checkbox"/> Elaborazione emittente	<input type="checkbox"/> Elaborazione pagamento – Internet
<input type="checkbox"/> Servizi di back-office	<input type="checkbox"/> Programmi di fedeltà	<input type="checkbox"/> Elaborazione pagamento – POS
<input type="checkbox"/> Gestione fatturazione	<input type="checkbox"/> Servizi gestiti	<input type="checkbox"/> Servizi prepagati
<input type="checkbox"/> Compensazione contabilizzazione e	<input type="checkbox"/> Servizi esercenti	<input type="checkbox"/> Gestione registrazioni
<input type="checkbox"/> Preparazione dati	<input type="checkbox"/> Provider di rete/Trasmettitore	<input type="checkbox"/> Pagamenti pubblici/fiscali
<input type="checkbox"/> Servizi di storno di addebito e frode	<input type="checkbox"/> Gateway/Switch di pagamento	
<input type="checkbox"/> Altro (specificare):		

Parte 2c. 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, ecc.)? Sì No

Parte 2d. Elaborazione delle transazioni

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

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

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

Parte 3. Convalida PCI DSS

In base ai risultati del questionario SAQ D datato (*data di compilazione SAQ*), (*ragione sociale provider di servizi*) 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 (*ragione sociale provider di servizi*) 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 (*ragione sociale provider di servizi*) 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 (*indicare numero di versione*), 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 ↑

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.*

⁵ 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.

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.

Requisito PCI DSS	Descrizione del requisito	Stato di conformità (selezionare una risposta)		Data e azioni di correzione (in caso di non conformità)
		SÌ	NO	
1	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati dei titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	<input type="checkbox"/>	<input type="checkbox"/>	
5	Utilizzare e aggiornare regolarmente il software antivirus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Sviluppare e gestire sistemi e applicazioni protette	<input type="checkbox"/>	<input type="checkbox"/>	
7	Limitare l'accesso ai dati 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 dei 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	Eeguire regolarmente test dei sistemi e processi di protezione	<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 D

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

Data di completamento:

Sviluppo e gestione di una rete sicura

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

Domanda PCI DSS		Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
1.1	Sono stabiliti standard di configurazione del firewall e del router che includano:				
1.1.1	È presente 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	(a) È presente un diagramma di rete aggiornato (ad esempio, un diagramma che illustra i flussi dei dati di titolari di carta attraverso la rete) che documenti tutte le connessioni ai dati di titolari di carta, compresa qualsiasi rete wireless?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il diagramma viene aggiornato?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	(a) Gli standard di configurazione del firewall comprendono i requisiti per un firewall per ogni connessione Internet e tra la zona DMZ e la zona della rete interna?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il diagramma di rete aggiornato è coerente con gli standard di configurazione del firewall?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Gli standard di configurazione di firewall e router comprendono una descrizione dei gruppi, dei ruoli e delle responsabilità per la gestione logica dei componenti della rete?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	(a) Gli standard di configurazione del firewall e del router includono un elenco documentato di servizi, protocolli e porte necessari per l'azienda, ad esempio i protocolli HTTP (Hypertext Transfer Protocol) e SSL (Secure Sockets Layer), SSH (Secure Shell) e VPN (Virtual Private Network)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono necessari tutti i servizi, protocolli e porte non sicuri consentiti e le funzioni di sicurezza sono documentate ed implementate per ciascuno di essi? <i>Nota: Esempi di servizi, protocolli o porte non sicuri includono, senza limitazioni, FTP, Telnet, POP3, IMAP e SNMP.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	(a) Gli standard di configurazione di firewall e router richiedono una revisione dei set di regole del firewall e del router almeno ogni sei mesi?		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		<u>Sì</u>	<u>No</u>	<u>Speciale*</u>
	(b) La revisione dei set di regole di firewall e router viene effettuata almeno ogni sei mesi?	<input type="checkbox"/>	<input type="checkbox"/>			
1.2	<p>Le configurazioni di firewall e router limitano le connessioni tra le reti non attendibili e qualsiasi sistema nell'ambiente dei dati di titolari di carta nel modo seguente:</p> <p><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></p>					
1.2.1	(a) Il traffico in entrata e in uscita è limitato a quello necessario per l'ambiente dei dati di titolari di carta e le restrizioni sono documentate?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Il resto del traffico in entrata e in uscita è negato in modo specifico (ad esempio utilizzando un comando esplicito "deny all" o un comando implicito di negazione dopo un'istruzione "allow")?	<input type="checkbox"/>	<input type="checkbox"/>			
1.2.2	Viene effettuata la protezione e sincronizzazione dei file di configurazione del router?	<input type="checkbox"/>	<input type="checkbox"/>			
1.2.3	Sono installati i firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e tali firewall sono configurati per negare o controllare il traffico (se necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3	La configurazione firewall vieta l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta, come segue:					
1.3.1	È implementata una zona DMZ per limitare il traffico in entrata ai soli componenti di sistema che forniscono servizi, protocolli e porte autorizzati accessibili pubblicamente?	<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	Sono stati vietati i percorsi diretti per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.4	Sono vietati gli indirizzi interni da Internet alla zona DMZ?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.5	Viene autorizzato in modo esplicito il traffico in uscita dall'ambiente dei dati di titolari di carta ad Internet?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.6	È stato implementato un controllo efficiente, anche noto come "dynamic packet filtering" (ossia, che consente solo alle connessioni già "stabilite" di accedere alla rete)?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.7	I componenti di sistema che memorizzano dati dei titolari di carta (come un database) sono collocati in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili?	<input type="checkbox"/>	<input type="checkbox"/>			

Domanda PCI DSS	Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale*</u>
1.3.8	(a) Sono in atto misure volte ad impedire la divulgazione di indirizzi IP privati ed informazioni di routing ad Internet? Nota: i metodi per oscurare l'indirizzamento IP possono includere, senza limitazioni: <ul style="list-style-type: none"> • NAT (Network Address Translation) • Posizionamento di server contenenti dati dei titolari di carta dietro server/firewall proxy o cache contenuti, • Rimozione o filtraggio di annunci di instradamento per reti private che utilizzano indirizzamento registrato, • Uso interno di spazio indirizzi RFC1918 invece degli indirizzi registrati. 	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono autorizzate eventuali divulgazioni ad entità esterne di indirizzi IP privati e di informazioni di routing?	<input type="checkbox"/>	<input type="checkbox"/>	
1.4	(a) Il firewall personale (software) è 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"/>	
	(b) Il software del firewall personale è configurato in base a standard specifici ed in modo che non possa essere modificato da utenti di computer portatili e/o di proprietà dei dipendenti?	<input type="checkbox"/>	<input type="checkbox"/>	

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

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
2.1	I valori predefiniti del fornitore vengono sempre modificati prima di installare un sistema in rete? <i>Le impostazioni predefinite del fornitore comprendono, senza limitazione, password, stringhe di comunità SNMP (Simple Network Management Protocol) ed eliminazione di account non necessari.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, sono stati modificati i valori predefiniti come segue:			
	(a) Sono state modificate le chiavi di cifratura predefinite al momento dell'installazione e vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono state modificate le stringhe di comunità SNMP predefinite sui dispositivi wireless?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Sono state modificate le password/passphrase predefinite sui punti di accesso?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) È aggiornato il firmware sui dispositivi wireless per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless?	<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Sono stati sviluppati standard di configurazione per tutti i componenti di sistema e sono coerenti con gli standard di System Hardening che sono accettati dal settore? Fonti di standard di System Hardening accettati dal settore possono comprendere, senza limitazione, enti quali SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) e Center for Internet Security (CIS).	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono aggiornati gli standard di configurazione del sistema in caso di identificazione di nuovi problemi di vulnerabilità, secondo quanto definito al Requisito 6.2?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Quando si configurano nuovi sistemi vengono applicati gli standard di configurazione del sistema?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Gli standard di configurazione del sistema comprendono quanto segue:			
2.2.1	(a) È implementata una sola funzione primaria per server, per evitare la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza? Ad esempio, server Web, database server e DNS devono essere implementati su server separati.	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
	(b) In caso di utilizzo di tecnologie di virtualizzazione, viene implementata una sola funzione primaria per dispositivo o componente di sistema virtuale?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	(a) Sono abilitati solo i servizi, protocolli, daemon ecc. necessari come richiesto per la funzione del sistema (sono disabilitati i servizi e protocolli che non sono strettamente necessari per eseguire la funzione specifica di un dispositivo)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono giustificati tutti i servizi, daemon o protocolli non sicuri abilitati e sono documentate ed implementate le funzioni di sicurezza? <i>(Ad esempio, tecnologie sicure come SSH, S-FTP, SSL, o IPsec VPN sono usate per proteggere servizi non sicuri come NetBIOS, file-sharing, Telnet, FTP, ecc).</i>	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	(a) Gli amministratori di sistema e/o il personale che si occupa della configurazione dei componenti di sistema conoscono in modo approfondito le impostazioni dei parametri di sicurezza per i componenti di sistema in questione?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le impostazioni dei parametri di sicurezza comuni del sistema sono comprese negli standard di configurazione del sistema?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le impostazioni dei parametri di sicurezza sono impostate correttamente sui componenti di sistema?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	(a) 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"/>	
	(b) Tutte le funzioni abilitate sono documentate e supportano una configurazione sicura?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Sui componenti di sistema è presente solo funzionalità documentata?	<input type="checkbox"/>	<input type="checkbox"/>	
2.3	È stata eseguita la cifratura dell'accesso amministrativo non da console come segue: <i>Utilizzare tecnologie quali SSH, VPN o SSL/TLS per la gestione basata su Web e altre attività amministrative non da console.</i>			
	(a) È stata eseguita la cifratura di tutto l'accesso amministrativo non da console con cifratura avanzata e viene richiamato un sistema di cifratura avanzata prima della richiesta della password dell'amministratore?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I servizi di sistema ed i file di parametri sono configurati in modo da impedire l'uso di Telnet e di altri comandi di accesso remoto non sicuri?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) L'accesso amministratore alle interfacce di gestione basate su Web è cifrato con un metodo di crittografia avanzata?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		<u>Speciale</u>*
		<u>Si</u>	<u>No</u>	
2.4	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? <i>Vedere l'appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso per requisiti specifici che devono essere soddisfatti.</i>	<input type="checkbox"/>	<input type="checkbox"/>	

Protezione dei dati di titolari di carta

Requisito 3: Proteggere i dati di titolari di carta memorizzati

Domanda PCI DSS		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale</u> *
3.1	Le politiche per la conservazione e l'eliminazione dei dati sono implementate come segue:				
3.1.1	(a) Sono implementate le politiche per la conservazione e l'eliminazione dei dati e comprendono requisiti specifici per la conservazione dei dati dei titolari di carta come necessario per fini commerciali, legali e/o legislativi? <i>Ad esempio, è necessario conservare i dati dei titolari di carta per un periodo X per scopi aziendali Y.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le politiche e le procedure includono disposizioni per l'eliminazione sicura dei dati non più necessari per scopi legali, legislativi o aziendali, inclusa l'eliminazione dei dati di titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le politiche e le procedure includono disposizioni per ogni tipo di memorizzazione dei dati di titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) I processi e le procedure comprendono almeno uno dei seguenti elementi? <ul style="list-style-type: none"> • Un processo programmatico (automatico o manuale) per rimuovere, almeno su base trimestrale, i dati di titolari di carta memorizzati che superano i requisiti definiti nella politica per la conservazione dei dati • Requisiti per una revisione, realizzata almeno su base trimestrale, per verificare che i dati dei titolari di carta memorizzati non superano i requisiti definiti nella politica per la conservazione dei dati. 		<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Tutti i dati dei titolari di carta memorizzati soddisfano i requisiti contenuti nella politica per la conservazione dei dati?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2	(a) Per emittenti e/o società che supportano servizi di emissione e memorizzano dati sensibili di autenticazione, esiste una giustificazione aziendale per la memorizzazione di dati sensibili di autenticazione ed è che i dati siano protetti?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Per tutte le altre entità, se sono stati ricevuti ed eliminati dati sensibili di autenticazione, sono in atto 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)?				

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
3.2.1	<p>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.</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, e ▪ Codice di servizio <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</i></p>	<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	<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 repository dei dati, supporti digitali portatili, supporti di backup e i log di audit) utilizzando uno dei seguenti approcci?</p> <ul style="list-style-type: none"> ▪ Hash one-way basati su crittografia avanzata (l'hash deve essere dell'intero PAN) ▪ Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN) ▪ 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>Nota: per un utente non autorizzato è relativamente facile ricostruire i dati PAN originali se ha accesso alla versione troncata e hash del PAN. Nel caso in cui versioni troncata e hash dello stesso PAN siano presenti nell'ambiente di un'entità, andrebbero predisposti ulteriori controlli per verificare che non sia possibile correlare le versioni troncata e hash per ricostruire il PAN originale.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:	Si	No	Speciale*
3.4.1	Se si utilizza la cifratura su disco (anziché la cifratura del database a livello di file o colonna), l'accesso viene gestito come segue:				
	(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 crittografiche sono memorizzate in modo sicuro (ad esempio, su un supporto rimovibile adeguatamente protetto con controlli di accesso rigorosi)?	<input type="checkbox"/>	<input type="checkbox"/>		
	(c) I dati dei titolari di carta su supporti rimovibili sono cifrati in ogni posizione di memorizzazione? <i>Nota: se la cifratura su disco non è utilizzata per cifrare supporti rimovibili, sarà necessario rendere illeggibili i dati memorizzati sul supporto in questione utilizzando altri metodi.</i>	<input type="checkbox"/>	<input type="checkbox"/>		
3.5	Ogni chiave viene utilizzata per garantire la protezione dei dati di titolari di carta da divulgazione e uso improprio come segue: <i>Nota: questo requisito si applica anche alle key-encrypting key (KEK) utilizzate per proteggere le chiavi di crittografia dei dati. Tali KEK devono essere avanzate almeno quanto la chiave di crittografia dei dati.</i>				
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	(a) Le chiavi sono memorizzate in formato cifrato e le KEK sono memorizzate separatamente dalle chiavi di crittografia dei dati?	<input type="checkbox"/>	<input type="checkbox"/>		
	(b) 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	(a) Tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzati per la cifratura dei dati di titolari di carta sono completamente documentati e implementati?	<input type="checkbox"/>	<input type="checkbox"/>		
	(b) Solo per provider di servizi: In caso di condivisione con i clienti delle chiavi per la trasmissione o la memorizzazione di dati dei titolari di carta, viene fornita ai clienti la documentazione comprendente istruzioni dettagliate per la trasmissione, la memorizzazione e l'aggiornamento in modo sicuro delle chiavi dei clienti, in conformità ai successivi requisiti da 3.6.1 a 3.6.8?	<input type="checkbox"/>	<input type="checkbox"/>		
	(c) I processi e le procedure per la gestione delle chiavi sono implementati in modo da rendere necessario quanto segue:				
3.6.1	Le procedure per le chiavi di crittografia comprendono la generazione di chiavi avanzate?	<input type="checkbox"/>	<input type="checkbox"/>		
3.6.2	Le procedure per le chiavi di crittografia comprendono la distribuzione di chiavi di crittografia sicure?	<input type="checkbox"/>	<input type="checkbox"/>		

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
3.6.3	Le procedure per le chiavi di crittografia comprendono la memorizzazione di chiavi di crittografia sicure?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Le procedure per le chiavi di crittografia comprendono modifiche delle chiavi di crittografia per le chiavi giunte al termine del loro periodo di validità (ad esempio, una volta trascorso un periodo di tempo definito e/o dopo la produzione da parte di una determinata chiave di una quantità definita di testo di cifratura), come specificato dal fornitore dell'applicazione associato o dal proprietario delle chiavi, ed in base alle linee guida ed alle migliori pratiche del settore (ad esempio, NIST Special Publication 800-57)?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	(a) Le procedure per chiavi di crittografia comprendono il ritiro o la sostituzione (ad esempio: archiviazione, distruzione e/o revoca) delle chiavi di crittografia in caso di indebolimento dell'integrità della chiave (ad esempio, partenza di un dipendente a conoscenza di chiavi con testo in chiaro)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le procedure per le chiavi di crittografia comprendono la sostituzione di chiavi potenzialmente o effettivamente compromesse?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) In caso di conservazione di chiavi di crittografia ritirate o sostituite, queste chiavi vengono usate solo per fini di decifratura o verifica (non usate per operazioni di cifratura)?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Le procedure per le chiavi di crittografia comprendono "split knowledge" e controllo duale delle chiavi (ad esempio, in modo che per ricostruire l'intera chiave siano necessarie due o tre persone, ciascuna a conoscenza di una sola parte della stessa) per le operazioni di gestione delle chiavi con testo in chiaro? <i>Nota: Esempi di operazioni manuali di gestione delle chiavi includono, senza limitazioni: la generazione, la trasmissione, il caricamento, la memorizzazione e la distruzione delle chiavi.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Le procedure per le chiavi di crittografia comprendono la prevenzione di tentativi di sostituzione non autorizzata delle chiavi?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Ai custodi delle chiavi viene richiesto di riconoscere in modo formale (in forma scritta o elettronica) che accettano e confermano di conoscere le proprie responsabilità come custodi delle chiavi?	<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:		Speciale*
		Sì	No	
4.1	(a) Sono utilizzati protocolli di crittografia e sicurezza avanzati, quali SSL/TLS, SSH o IPSEC, per proteggere i dati sensibili di titolari di carta durante la trasmissione su reti pubbliche e aperte? <i>Esempi di reti pubbliche aperte che rientrano nell'ambito degli standard PCI DSS comprendono, senza limitazioni, la rete Internet, le tecnologie wireless, le reti GSM (Global System for Mobile communications) e le reti GPRS (General Packet Radio Service).</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Vengono accettati solo certificati e/o chiavi affidabili?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Sono implementati protocolli di sicurezza per usare solo configurazioni sicure e non supportare versioni o configurazioni non sicure?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Viene implementato il livello di cifratura corretto per la metodologia in uso (controllare i suggerimenti, le pratiche consigliate del fornitore)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Per le implementazioni SSL/TLS: <ul style="list-style-type: none"> L'HTTPS viene visualizzato come parte dell'URL del browser? I dati del titolare di carta sono richiesti solo quando l'HTTPS viene visualizzato nell'URL? 	<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	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? Nota: <i>l'utilizzo della tecnologia WEP per controllare la sicurezza è stato vietato a partire dal 30 giugno 2010.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	(a) I PAN sono resi illeggibili o sicuri con crittografia avanzata ogni volta che vengono inviati utilizzando tecnologie di messaggistica degli utenti finali (ad esempio e-mail, messaggistica istantanea o chat)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono in atto politiche in cui viene indicato che i PAN non protetti non si devono inviare mediante tecnologie di messaggistica degli utenti finali?	<input type="checkbox"/>	<input type="checkbox"/>	

Utilizzare un programma per la gestione delle vulnerabilità

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

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

Requisito 6: Sviluppare e gestire sistemi e applicazioni protette

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

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
6.2	<p>(a) Esiste un processo per identificare vulnerabilità della sicurezza recentemente rilevate, compresa una classificazione di rischio che viene assegnata a tali vulnerabilità? (Le vulnerabilità di rischio più elevato, più critiche dovrebbero essere classificate almeno come "Elevate").</p> <p>Nota: Le classificazioni di rischio si dovrebbero basare sulle migliori pratiche del settore. Ad esempio, i criteri per la classificazione di vulnerabilità di rischio "Elevato" possono comprendere un punteggio base CVSS di 4.0 o superiore e/o una patch del fornitore da questi classificata come "critica" e/o una vulnerabilità che interessa un componente di sistema critico.</p> <p><i>La classificazione delle vulnerabilità è considerata una delle migliori pratiche fino al 30 giugno 2012; dopo tale data, diventerà un requisito.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I processi per identificare le nuove vulnerabilità della sicurezza comprendono l'uso di fonti esterne per informazioni sulle vulnerabilità della sicurezza?	<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) I processi di sviluppo del software si fondano su migliori pratiche e/o standard di settore?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) La sicurezza delle informazioni è compresa per l'intera durata del ciclo di sviluppo del software?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le applicazioni software sono sviluppate in conformità agli standard PCI DSS (ad esempio autenticazione e registrazione sicure)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) I processi di sviluppo software garantiscono quanto segue?			
6.3.1	Account, ID utente e/o password di applicazioni personalizzate vengono rimossi prima dell'attivazione o della distribuzione di tali applicazioni ai clienti?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
6.3.2	<p>Tutte le modifiche del codice dell'applicazione personalizzata sono analizzate (utilizzando processi manuali o automatici) prima del rilascio in produzione o della distribuzione ai clienti per individuare eventuali vulnerabilità del codice come segue:</p> <ul style="list-style-type: none"> Le modifiche del codice vengono analizzate da utenti singoli diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure? L'analisi del codice garantisce che il codice venga sviluppato in base a linee guida di codifica sicure (come da requisito 6.5 PCI DSS)? Le correzioni appropriate vengono implementate prima del rilascio? I risultati dell'analisi del codice vengono esaminati e approvati dal management prima del rilascio? <p>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. Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. 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.</p>	<input type="checkbox"/>	<input type="checkbox"/>	
6.4	I processi e le procedure di controllo delle modifiche sono seguiti per tutte le modifiche apportate ai componenti di sistema per comprendere quanto segue:			
6.4.1	Gli ambienti di sviluppo/test sono separati dagli ambienti di produzione e sono in atto metodi di controllo dell'accesso per garantire la separazione di tali ambienti?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Esiste una separazione di responsabilità tra il personale assegnato agli ambienti di sviluppo/test e il personale assegnato all'ambiente di produzione?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	I dati di produzione (PAN attivi) non sono usati per le attività di test o sviluppo?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Vengono rimossi account e dati di test prima dell'attivazione dei sistemi di produzione?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5	(a) Sono documentate le procedure di controllo delle modifiche per implementare le patch di sicurezza e le modifiche al software e richiedono i successivi punti 6.4.5.1 – 6.4.5.4?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Viene eseguito quanto indicato di seguito per tutte le modifiche:			
6.4.5.1	Documentazione dell'impatto?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5.2	Approvazione documentata delle parti autorizzate?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5.3	(a) Test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
	(b) Per le modifiche del codice personalizzate, gli aggiornamenti vengono sottoposti a test per verificarne la conformità al Requisito 6.5 PCI DSS prima del rilascio in produzione?	<input type="checkbox"/>	<input type="checkbox"/>	
	6.4.5.4 Le procedure di back-out sono preparate per ogni modifica?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5	(a) Le applicazioni sono sviluppate in base a linee guida di codifica sicura? <i>(Ad esempio, la Guida OWASP (Open Web Application Security Project), la Top 25 SANS CWE, la Codifica sicura CERT, ecc.)?</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Gli sviluppatori sono esperti di tecniche di codifica sicura?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Nei processi di sviluppo del software è coperta la prevenzione di comuni vulnerabilità di codifica per garantire che le applicazioni non siano vulnerabili, come minimo, a quanto segue: <i>Nota: le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.9 erano presenti nelle migliori pratiche del settore al momento della pubblicazione di questa versione degli standard PCI DSS. Tuttavia, poiché le migliori pratiche del settore per la gestione delle vulnerabilità sono aggiornate, per questi requisiti devono essere usate le pratiche migliori attuali.</i>			
6.5.1	Injection flaw, in particolare SQL injection? (Convalidare l'input per verificare che i dati dell'utente non possono modificare il significato di comandi e query, utilizzare query parametrizzate, ecc). <i>Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Buffer overflow? (Convalidare limiti di buffer e troncatura stringhe di input).	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Memorizzazione di dati crittografici non sicura? (Evitare gli errori di crittografia).	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Comunicazioni non sicure? (Cifrare in modo appropriato tutte le comunicazioni autenticate e riservate).	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Gestione degli errori non corretta? (Non perdere informazioni mediante messaggi di errore).	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	6.5.6 Tutte le vulnerabilità "Elevate" individuate nel processo di identificazione delle vulnerabilità (come definito nel Requisito 6.2 PCI DSS)? <i>Nota: questo requisito è considerato una delle pratiche migliori fino al 30 giugno 2012; dopo tale data, diventerà un requisito</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	Per applicazioni web ed interfacce di applicazioni (interne o esterne) ci si occupa anche delle seguenti vulnerabilità aggiuntive:			
6.5.7	Cross-site scripting (XSS)? (Convalidare tutti i parametri prima dell'inclusione, utilizzando sblocco contestuale, ecc).	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Si	No	
6.5.8	Controllo di accesso non corretto come riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL e scansione trasversale directory? (Autenticare in modo corretto gli utenti e modificare input. Non esporre agli utenti riferimenti a oggetti interni).	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Cross-site request forgery (CSRF)? (Non considerare sicure credenziali di autorizzazione e token inviati automaticamente dai browser).	<input type="checkbox"/>	<input type="checkbox"/>	
6.6	<p>Per le applicazioni Web esterne, viene assicurata in modo costante la protezione da nuove minacce e vulnerabilità e queste applicazioni sono protette da attacchi noti applicando <i>uno</i> dei seguenti metodi?</p> <ul style="list-style-type: none"> ▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatici di valutazione della sicurezza della vulnerabilità delle applicazioni, come segue: <ul style="list-style-type: none"> ○ Almeno una volta all'anno ○ Dopo ogni modifica ○ Da un'organizzazione specializzata in sicurezza delle applicazioni ○ Che tutte le vulnerabilità vengano corrette ○ Che l'applicazione venga nuovamente valutata dopo le correzioni – o – ▪ Installando un firewall a livello di applicazioni Web davanti alle applicazioni Web rivolte al pubblico per rilevare ed evitare attacchi basati su Web. <p>Nota: per "organizzazione specializzata nella sicurezza delle applicazioni" si intende una società esterna o un'organizzazione interna specializzata nella sicurezza delle applicazioni e in grado di dimostrare indipendenza dal team di sviluppo.</p>	<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:		Speciale*
		Si	No	
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"/>	
7.1.3	È necessaria l'approvazione documentata delle parti autorizzate (in forma scritta o elettronica) che specifica i privilegi richiesti?	<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Sono implementati i controlli dell'accesso tramite un sistema automatico di controllo dell'accesso?	<input type="checkbox"/>	<input type="checkbox"/>	
7.2	Per sistemi con più utenti, è presente un meccanismo di controllo dell'accesso per limitarlo in base alla reale necessità di un utente ed è impostato su "deny all" per impedire ogni accesso se non specificatamente consentito, come segue:			
7.2.1	Sono presenti sistemi di controllo dell'accesso su tutti i componenti di sistema?	<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	I sistemi di controllo dell'accesso sono configurati in modo che i privilegi vengano assegnati agli utenti in base alla classificazione e alla funzione del ruolo?	<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	I sistemi di controllo dell'accesso dispongono di un'impostazione predefinita "deny-all"? <i>Nota: alcuni sistemi di controllo dell'accesso sono impostati in modo predefinito su "allow-all" consentendo, pertanto, l'accesso a meno che/finché non viene scritta una regola per negare l'accesso in modo specifico.</i>	<input type="checkbox"/>	<input type="checkbox"/>	

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

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
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"> ▪ Qualcosa che l'utente conosce, come una password o una passphrase ▪ Qualcosa in possesso dell'utente, come un dispositivo token o una smart card ▪ Qualcosa che l'utente è, come biometrico 	<input type="checkbox"/>	<input type="checkbox"/>	
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>(Ad esempio, RADIUS (Remote Authentication and Dial-in Service) con token; TACACS (Terminal Access Controller Access Control System) con token; oppure altre tecnologie che facilitano l'autenticazione a due fattori).</i> Nota: l'autenticazione a due fattori richiede l'utilizzo di due dei tre metodi di autenticazione (fare riferimento al Requisito 8.2 per le descrizioni dei metodi di autenticazione). Usare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a due fattori.	<input type="checkbox"/>	<input type="checkbox"/>	
8.4	(a) Tutte le password sono rese illeggibili durante la trasmissione e la memorizzazione su tutti i componenti di sistema utilizzando crittografia avanzata?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Solo per provider di servizi: Le password dei clienti sono crittografate?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5	Sono presenti controlli per la gestione di autenticazioni e password utente per utenti non consumatori e amministratori in tutti i componenti del sistema, come segue:			
8.5.1	Le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi sono controllate, in modo che gli ID utente siano implementati solo come autorizzati (incluso con privilegi specificati)?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	Viene verificata l'identità dell'utente prima di eseguire il ripristino della password per le richieste presentate dagli utenti in forma non diretta (ad esempio via telefono, e-mail o Web)?	<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 disattivato o rimosso immediatamente?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	Gli account utente non attivi per oltre 90 giorni vengono rimossi o disattivati?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
8.5.6	(a) Gli account utilizzati dai fornitori per l'accesso, la manutenzione o l'assistenza in remoto sono abilitati solo durante il periodo di tempo necessario?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Gli account per l'accesso in remoto dei fornitori vengono monitorati mentre sono in uso?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Le procedure e le politiche di autenticazione vengono comunicate a tutti gli utenti con accesso ai dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	Account e password di gruppo, condivisi o generici o altri metodi di autenticazione sono vietati come segue: <ul style="list-style-type: none"> • Gli ID e gli account utente generici sono disabilitati o rimossi; • Non esistono ID utente condivisi per le attività di amministrazione del sistema e per altre funzioni critiche; e • Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema 	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	(a) Le password utente sono modificate almeno ogni 90 giorni?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Solo per provider di servizi: È necessaria la modifica periodica delle password per utenti non consumatori e a tali utenti vengono fornite tutte le informazioni necessarie relativamente a quando ed in quali circostanze occorre modificare le password?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	(a) La lunghezza minima della password è impostata su 7 caratteri?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Solo per provider di servizi: Le password per utenti non consumatori devono soddisfare i requisiti di lunghezza minima?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	(a) Le password devono contenere caratteri numerici e alfabetici?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Solo per provider di servizi: Le password per utenti non consumatori devono contenere caratteri numerici ed alfabetici?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	(a) La nuova password specificata deve essere diversa dalle ultime quattro password utilizzate?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Solo per provider di servizi: Le nuove password per utenti non consumatori devono essere diverse dalle ultime quattro password utilizzate?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	(a) I tentativi di accesso ripetuti sono limitati bloccando l'ID utente dopo un massimo di sei tentativi?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Solo per provider di servizi: È previsto il blocco temporaneo delle password per utenti non consumatori dopo un massimo di sei tentativi di accesso non riusciti?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		<u>Speciale</u> *
		<u>Sì</u>	<u>No</u>	
8.5.14	Una volta che un account utente è bloccato, la durata del blocco è impostata almeno su 30 minuti oppure 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, agli utenti viene richiesto di effettuare nuovamente l'autenticazione (ad esempio immettere di nuovo la password) per riattivare il terminale o la sessione?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	(a) Ogni accesso a database contenenti i dati di titolari di carta è autenticato? (Ciò comprende gli accessi da applicazioni, amministratori e tutti gli altri utenti).	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Tutti gli accessi, le query e le azioni dell'utente (ad esempio, spostamento, copia, eliminazione) sul database si verificano solo tramite metodi programmatici (ad esempio, procedure memorizzate)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) L'accesso diretto utente o le query ai database è limitato solo agli amministratori del database?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Gli ID di applicazione con accesso al database possono essere usati solo dalle applicazioni (e non da singoli utenti o altri processi)?	<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> *
9.1	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) Sono presenti videocamere e/o altri meccanismi di controllo dell'accesso 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) Le videocamere e/o gli altri meccanismi di controllo dell'accesso sono protetti da manomissione o disattivazione?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) I dati raccolti dalle videocamere e/o da altri meccanismi di controllo dell'accesso sono controllati e correlati ad altri dati, inoltre tali dati vengono memorizzati per almeno tre mesi, se non diversamente richiesto dalla legge?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.2	L'accesso fisico a connettori di rete accessibili pubblicamente è limitato (ad esempio, nelle aree accessibili ai visitatori non devono essere attivate porte di rete a meno che l'accesso alla rete non sia espressamente autorizzato)? In alternativa, vengono scortati costantemente i visitatori nelle aree con connettori di rete attivi?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	Viene limitato l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione?		<input type="checkbox"/>	<input type="checkbox"/>	
9.2	Le procedure sono elaborate per consentire di distinguere facilmente tra personale in sede e visitatori, come segue <i>Ai fini del Requisito 9, per "personale in sede" si intendono le persone assunte a tempo pieno o part-time, le persone con contratto a tempo determinato, i collaboratori o i consulenti che sono fisicamente presenti presso i locali dell'entità. Per "visitatore" si intende un fornitore, un ospite del personale in sede, un tecnico dell'assistenza o chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente per non più di un giorno.</i>				
	(a) I processi e le procedure per l'assegnazione delle tessere magnetiche a dipendenti e visitatori includono quanto segue: <ul style="list-style-type: none"> • Concessione di nuove tessere magnetiche, • Modifica dei requisiti di accesso, e • Revoca per il personale in sede che ha lasciato l'azienda e tessere magnetiche per visitatori scadute? 		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
	(b) L'accesso al sistema di tessere magneti è limitato al personale autorizzato?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le tessere magnetiche identificano chiaramente i visitatori e consentono una facile distinzione tra personale in sede visitatori?	<input type="checkbox"/>	<input type="checkbox"/>	
9.3	Tutti i visitatori sono gestiti nel seguente modo:			
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	(a) I visitatori ricevono un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) che li identifica non come personale in sede?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le tessere magnetiche hanno una scadenza?	<input type="checkbox"/>	<input type="checkbox"/>	
9.3.3	Ai visitatori viene richiesta la restituzione del token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza?	<input type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) Viene utilizzato un registro dei visitatori per registrare gli accessi fisici alla struttura nonché alle aree computer e ai centri dati in cui vengono memorizzati o trasmessi i dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il registro dei visitatori contiene il nome del visitatore, l'azienda rappresentata ed il personale in sede che autorizza l'accesso fisico? Tale registro viene conservato almeno per tre mesi?	<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 di questa sede viene controllata almeno una volta all'anno?	<input type="checkbox"/>	<input type="checkbox"/>	
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 includono 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"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
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"/>	
9.9.1	I registri di inventario per tutti i supporti sono conservati in modo adeguato e si eseguono gli inventari dei supporti periodici almeno una volta l'anno?	<input type="checkbox"/>	<input type="checkbox"/>	
9.10	Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?	<input type="checkbox"/>	<input type="checkbox"/>	
	La distruzione avviene in base alle seguenti modalità:			
9.10.1	(a) I materiali cartacei sono distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo da rendere impossibile la ricostruzione dei dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I contenitori usati per conservare le informazioni da distruggere sono protetti per impedire l'accesso al contenuto? (Ad esempio, un contenitore per "informazioni da distruggere" dispone di un dispositivo di blocco che impedisce l'accesso al contenuto).	<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Si rendono irrecuperabili i dati di titolari di carta su supporti elettronici tramite un programma di pulizia basato su standard di settore accettati per l'eliminazione sicura oppure in altro modo attraverso la distruzione fisica dei supporti (ad esempio, smagnetizzandoli) in modo da rendere impossibile la ricostruzione dei dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	

Monitoraggio e test delle reti regolari

Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
10.1	È previsto un processo per collegare ogni 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 del dato interessato, componente di sistema o risorsa?	<input type="checkbox"/>	<input type="checkbox"/>	
10.4	(a) Tutti gli orologi e gli orari critici del sistema sono sincronizzati utilizzando la tecnologia per la sincronizzazione dell'ora? Tale tecnologia viene aggiornata? <i>Nota: NTP (Network Time Protocol) rappresenta un esempio di tecnologia per la sincronizzazione dell'ora.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Sono implementati i seguenti controlli per l'acquisizione, la distribuzione e la memorizzazione dell'ora:			
10.4.1	(a) Sono solo i server di rilevamento dell'orario centrali a ricevere i segnali orari da risorse esterne e tutti i sistemi critici hanno l'ora esatta e coerente, sulla base di International Atomic Time o UTC?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I server di rilevamento dell'orario centrali designati comunicano tra loro per mantenere l'ora esatta e gli altri server interni ricevono l'ora solo dai server centrali?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:	Si	No	Speciale*
10.4.2	I dati dell'ora sono protetti come segue: (a) L'accesso ai dati dell'ora è limitato solo al personale con un'esigenza aziendale di accedere a tali dati? (b) Le modifiche alle impostazioni dell'ora su sistemi critici sono registrate, monitorate ed esaminate?		<input type="checkbox"/>	<input type="checkbox"/>	
10.4.3	Le impostazioni dell'ora sono ricevute da fonti specifiche accettate dal settore? (Ciò al fine di evitare la modifica dell'ora da parte di utenti non autorizzati). Facoltativamente, tali aggiornamenti possono essere cifrati con una chiave simmetrica ed è possibile creare elenchi di controllo dell'accesso che specifichino gli indirizzi IP dei computer client ai quali verranno forniti gli aggiornamenti di ora (per evitare un uso non autorizzato dei server di rilevamento dell'ora interni).		<input type="checkbox"/>	<input type="checkbox"/>	
10.5	Gli audit trail sono protetti in modo che non possano essere modificati, come 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 in modo da non consentire modifiche non autorizzate tramite meccanismi di controllo dell'accesso, separazione fisica e/o di rete?		<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"/>	
10.5.4	I registri per le tecnologie rivolte al pubblico (ad esempio, wireless, firewall, DNS, e-mail) vengono scaricati e copiati su un server di registro centralizzato sicuro o su una 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 registri per tutti i componenti di sistema sono esaminati almeno una volta al giorno e sono necessari gli interventi per le eccezioni? <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> Nota: è consentito l'uso degli strumenti di raccolta, analisi e generazione di avvisi per i log ai fini della conformità al requisito 10.6.		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	(a) Sono presenti politiche e procedure per la conservazione del registro di audit e prevedono la conservazione della cronologia dell'audit trail per almeno un anno?		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS	Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
(b) I registri di audit sono disponibili per almeno un anno e sono presenti processi per recuperare immediatamente i registri almeno degli ultimi tre mesi per consentirne un'analisi immediata?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Domanda PCI DSS	Risposta:	<u>Sì</u>	<u>No</u>	<u>Speciale</u> *
11.1 (a) È implementato un processo documentato per rilevare ed identificare i punti di accesso wireless su base trimestrale? <i>Nota: i metodi che si possono utilizzare nel processo comprendono, senza limitazioni, scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless. Qualunque sia il metodo adottato, questo deve essere in grado di rilevare ed identificare qualsiasi dispositivo non autorizzato.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
(b) La metodologia rileva ed identifica ogni punto di accesso wireless non autorizzato, compreso, come minimo, quanto segue: <ul style="list-style-type: none"> • Schede WLAN inserite nei componenti di sistema; • Dispositivi portatili wireless collegati a componenti di sistema (ad esempio, via USB, ecc.); • Dispositivi wireless collegati ad una porta o a un dispositivo di rete? 		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Il processo per identificare punti di accesso wireless non autorizzati viene eseguito con cadenza trimestrale per tutte le strutture e i componenti di sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
(d) In caso di utilizzo di monitoraggio automatico (ad esempio, IDS/IPS wireless, NAC, ecc.), tale monitoraggio è configurato per generare avvisi per il personale?		<input type="checkbox"/>	<input type="checkbox"/>	
(e) Il piano di risposta agli incidenti (Requisito 12.9) comprende una risposta in caso di rilevamento di dispositivi wireless non autorizzati?		<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
11.2	<p>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), come segue?</p> <p>Nota: non è necessario completare quattro scansioni trimestrali per la conformità iniziale a PCI DSS, nel caso in cui 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) ogni vulnerabilità rilevata dalla scansione è stata corretta come dimostrato da una nuova scansione. Per gli anni successivi alla scansione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.</p>			
11.2.1	(a) Vengono eseguite scansioni interne di vulnerabilità trimestrali?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il processo di scansioni interne trimestrali comprende nuove scansioni fino al conseguimento di risultati positivi, oppure fino alla risoluzione di tutte le vulnerabilità "Elevate" in base alla definizione contenuta nel Requisito 6.2 PCI DSS?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le scansioni interne trimestrali sono eseguite da una risorsa interna o da una terza parte qualificata e, se applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	
11.2.2	(a) Vengono eseguite scansioni esterne di vulnerabilità trimestrali?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I risultati delle scansioni esterne trimestrali soddisfano i requisiti della Guida del programma per i fornitori di scansioni approvati (ad esempio nessuna vulnerabilità classificata superiore a 4.0 dal CVSS e nessun errore automatico)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le scansioni esterne delle vulnerabilità trimestrali sono eseguite da un fornitore di scansioni approvato (ASV) e autorizzato da PCI SSC?	<input type="checkbox"/>	<input type="checkbox"/>	
11.2.3	<p>(a) Le scansioni interne ed esterne della rete vengono eseguite dopo ogni cambiamento significativo (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)?</p> <p>Nota: le scansioni realizzate dopo le modifiche della rete possono essere eseguite da personale interno.</p>	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		Speciale*
		Sì	No	
	(b) Il processo di scansione comprende nuove scansioni fino a quando: <ul style="list-style-type: none"> Per le scansioni esterne, non esistano vulnerabilità a cui sia assegnato un punteggio superiore a 4.0 da parte del CVSS, Per le scansioni interne, sia stato conseguito un risultato positivo oppure siano state risolte tutte le vulnerabilità "Elevate" in base alla definizione contenuta nel Requisito 6.2 PCI DSS? 	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Le scansioni sono eseguite da una risorsa interna o da una terza parte qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<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 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) Vengono corrette le vulnerabilità rilevate sfruttabili e il test viene ripetuto?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) I test sono eseguiti da una risorsa interna o da una terza parte qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione(non necessariamente un QSA o un ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	
	I test di penetrazione includono quanto segue:			
11.3.1	Test di penetrazione a livello di rete? <i>Nota: tali test devono includere i componenti che supportano le funzioni di rete nonché i sistemi operativi.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Test di penetrazione a livello di applicazione? <i>Nota: i test devono includere almeno le vulnerabilità elencate nel Requisito 6.5.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
11.4	(a) Sono utilizzati sistemi di rilevamento e/p prevenzione delle intrusioni per monitorare tutto il traffico in corrispondenza del perimetro dell'ambiente dei dati di titolari di carta nonché presso i punti critici all'interno dell'ambiente stesso?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) I dispositivi IDS e/o IPS sono configurati per segnalare possibili compromissioni al personale?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Vengono tenuti aggiornati tutti i sistemi, le basi e le firme di rilevamento e prevenzione delle intrusioni?	<input type="checkbox"/>	<input type="checkbox"/>	

Domanda PCI DSS		Risposta:		<u>Si</u>	<u>No</u>	<u>Speciale</u> *
11.5	<p>(a) Gli strumenti per il monitoraggio dell'integrità dei file sono distribuiti all'interno dell'ambiente dei dati dei titolari di carta?</p> <p>Tra gli esempi di file che devono essere monitorati:</p> <ul style="list-style-type: none"> • Eseguibili di sistema • Eseguibili di applicazioni • File di configurazione e parametri • File memorizzati centralmente, di cronologia o archiviazione, di registro e audit 	<input type="checkbox"/>	<input type="checkbox"/>			
	<p>(b) Gli strumenti sono configurati per segnalare al personale modifiche non autorizzate di file system, file di configurazione o file di contenuto critici? Questi strumenti eseguono confronti di file critici almeno una volta alla settimana?</p> <p>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).</p>	<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:		Speciale*
		Si	No	
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"/>	
12.1.1	La politica risponde a tutti i requisiti PCI DSS?	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	(a) È documentato un processo per la valutazione dei rischi annuale che individua minacce e vulnerabilità e che consente di ottenere una valutazione formale dei rischi? (Esempi di metodologie per la valutazione dei rischi includono, senza limitazioni, OCTAVE, ISO 27005 e NIST SP 800-30).	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Il processo per la valutazione dei rischi viene eseguito con cadenza almeno annuale?	<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"/>	
12.2	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) e le stesse contemplano procedure tecniche ed amministrative per ciascun requisito?	<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? Richiedono quanto segue:			
12.3.1	Approvazione esplicita delle parti autorizzate per l'uso delle tecnologie?	<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 per determinare 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"/>	

Domanda PCI DSS		Risposta:	Si	No	Speciale*
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 fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.10	(a) Per il personale che ha accesso ai dati di titolari di carta tramite tecnologie di accesso remoto, la politica specifica il divieto di copiare, spostare o memorizzare tali dati su dischi rigidi locali e supporti elettronico rimovibili salvo espressa autorizzazione per una specifica esigenza aziendale?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Per il personale in possesso di opportuna autorizzazione, la politica richiede la protezione dei dati dei titolari di carta in conformità ai Requisiti PCI DSS?		<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	La responsabilità di protezione delle informazioni è assegnata in modo formale ad un CSO (Chief Security Officer) o a un altro membro del management esperto in sicurezza?		<input type="checkbox"/>	<input type="checkbox"/>	
	Le seguenti responsabilità per la gestione della sicurezza delle informazioni sono state assegnate 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	(a) È presente un programma formale di consapevolezza della sicurezza per rendere tutto il personale consapevole dell'importanza della sicurezza dei dati di titolari di carta?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le procedure inserite nel programma di consapevolezza della sicurezza comprendono quanto segue:				

Domanda PCI DSS		Risposta:		Si	No	Speciale*
12.6.1	(a) Il programma di consapevolezza della sicurezza mette a disposizione diversi strumenti di comunicazione e formazione dei dipendenti (ad esempio, poster, lettere, promemoria, formazione basata su Web, riunioni e promozioni)? <i>Nota: i metodi possono essere diversi in funzione del ruolo svolto dal personale e del loro livello di accesso ai dati dei titolari di carta.</i>	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) È prevista la formazione del personale al momento dell'assunzione ed almeno una volta all'anno?	<input type="checkbox"/>	<input type="checkbox"/>			
12.6.2	Al personale viene richiesto di certificare, almeno una volta all'anno, di aver letto e compreso la politica e le procedure di sicurezza?	<input type="checkbox"/>	<input type="checkbox"/>			
12.7	Il personale potenziale (fare riferimento alla definizione di "personale" di cui al precedente Requisito 12.1) viene sottoposto a screening prima dell'assunzione per ridurre al minimo il rischio di attacchi da fonti interne? Esempi di indagini sulla storia personale sono informazioni su impieghi precedenti, precedenti penali, storico del credito e controlli delle referenze. <i>Nota: questo requisito è solo consigliato per il personale potenziale che viene assunto per determinate posizioni come cassieri di negozi, con accesso a un solo numero di carta alla volta durante una transazione.</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 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"/>			
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 con cadenza almeno annuale?	<input type="checkbox"/>	<input type="checkbox"/>			
12.9	È stato implementato un piano di risposta in preparazione alla risposta immediata a una violazione del sistema che includa quanto segue:					
12.9.1	(a) È stato creato un piano di risposta da implementare in caso di violazione del sistema?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Il piano include 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"/>			

Domanda PCI DSS		Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale</u> *
	<ul style="list-style-type: none"> ▪ Procedure specifiche di risposta agli incidenti? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> ▪ Procedure di ripristino e continuità delle attività aziendali? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> ▪ Processi di backup dei dati? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> ▪ Analisi dei requisiti legali per la segnalazione di violazioni? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> ▪ Copertura e risposte per tutti i componenti di sistema critici? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> ▪ 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	Nel piano di risposta agli incidenti sono 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 PCI DSS	Risposta:	Sì	No	Speciale*
A.1	<p>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, come segue:</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	<p>Ogni entità esegue processi con accesso esclusivo al proprio ambiente dei dati di titolari di carta? I processi di tali applicazioni sono eseguiti utilizzando l'ID univoco assegnato all'entità?</p> <p>Ad esempio:</p> <ul style="list-style-type: none"> Nessuna entità nel sistema può utilizzare un ID utente di un server Web condiviso. Tutti gli script CGI utilizzati dall'entità devono essere creati ed eseguiti con l'ID utente univoco dell'entità 		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	<p>L'accesso e i privilegi di ciascuna entità sono limitati al relativo ambiente di dati di titolari di carta, come segue:</p>				
	(a) Gli ID utente per i processi dell'applicazione non sono utenti privilegiati (root/amministratore)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Ogni entità dispone di diritti di lettura, scrittura o esecuzione solo per i propri file e directory o per i system file necessari (tramite autorizzazione su file system, elenchi di controllo degli accessi, funzioni chroot o jailshell, ecc.)?		<input type="checkbox"/>	<input type="checkbox"/>	
	<i>Importante: i file di un'entità non possono essere condivisi per gruppi.</i>				
	(c) Tutti gli utenti di un'entità non hanno accesso in scrittura a file di sistema binari condivisi?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) La visualizzazione delle voci di registro è consentita solo all'entità proprietaria?		<input type="checkbox"/>	<input type="checkbox"/>	

	Domanda PCI DSS	Risposta:	<u>Si</u>	<u>No</u>	<u>Speciale</u>*
	<p>(e) Vengono applicate limitazioni all'utilizzo di queste risorse di sistema?</p> <ul style="list-style-type: none"> • Spazio sul disco, • Larghezza di banda, • Memoria, • CPU <p><i>Ciò assicura che un'entità non possa monopolizzare le risorse del server per sfruttarne le vulnerabilità (condizioni di errore, "race" e riavvio che generano, ad esempio, buffer overflow)</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	<p>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?</p> <p>La generazione dei registri è abilitata come segue per ogni ambiente di esercente e provider di servizi:</p>		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> • I registri sono abilitati per applicazioni di terze parti comuni? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> • I registri sono attivi per impostazione predefinita? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> • I registri sono disponibili per la revisione da parte dell'entità proprietaria? 		<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> • Le posizioni dei registri sono comunicate in modo chiaro all'entità proprietaria? 		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	<p>Sono abilitati processi e politiche in forma scritta 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?</p>		<input type="checkbox"/>	<input type="checkbox"/>	

Appendice B: Controlli compensativi

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

I controlli compensativi devono soddisfare i seguenti criteri:

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

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

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

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

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

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

Appendice C: Foglio di lavoro - Controlli compensativi

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

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

Numero e definizione del requisito:

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

Foglio di lavoro Controlli compensativi - Esempio

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

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

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

