



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

# **Questionario di autovalutazione A e Attestato di conformità**

---

**Nessuna memorizzazione, elaborazione o  
trasmissione dati di titolari di carte in formato  
elettronico**

**Versione 1.2**

Ottobre 2008

## 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. |
|                |          |  |
|                |          |  |
|                |          |  |

## Sommario

---

|  |            |
|--|------------|
| <b>Modifiche del documento .....</b>   | <b>i</b>   |
| <b>PCI DSS: Documenti correlati .....</b>  | <b>ii</b>  |
| <b>Operazioni preliminari .....</b>  | <b>iii</b> |
| <b>Completamento del questionario di autovalutazione.....</b>  | <b>iii</b> |
| <b>Conformità agli standard PCI DSS – Operazioni .....</b>   | <b>iii</b> |
| <b>Guida per la non applicabilità di determinati requisiti specifici .....</b>   | <b>iii</b> |
| <b>Attestato di conformità, SAQ A.....</b>   | <b>1</b>   |
| <b>Questionario di autovalutazione A .....</b>   | <b>4</b>   |
| <b>Implementazione di rigide misure di controllo dell'accesso .....</b>  | <b>4</b>   |
| <i>Requisito 9: Limitare l'accesso fisico ai dati di titolari di carta .....</i>   | <i>4</i>   |
| <b>Gestire una politica di sicurezza delle informazioni .....</b>  | <b>5</b>   |
| <i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori.....</i> | <i>5</i>   |
| <b>Appendice A: (non utilizzata) .....</b>   | <b>6</b>   |
| <b>Appendice B: Controlli compensativi.....</b>  | <b>7</b>   |
| <b>Appendice C: Foglio di lavoro - Controlli compensativi.....</b>   | <b>8</b>   |
| <b>Foglio di lavoro Controlli compensativi - Esempio .....</b>   | <b>9</b>   |
| <b>Appendice D: Spiegazione di non applicabilità:.....</b>   | <b>10</b>  |

## PCI DSS: Documenti correlati

---

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

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

---

<sup>1</sup> 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 A è stato sviluppato per rispondere ai requisiti applicabili ad esercenti che conservano solo resoconti o ricevute cartacee con i dati di titolari di carta e non i dati stessi in formato elettronico e che non elaborano o trasmettono tali dati in loco.

*Gli esercenti, così come definiti nel Tipo di convalida SAQ 1 e nel documento PCI DSS: Istruzioni e linee guida per l'autovalutazione, non memorizzano i dati di titolari di carta in formato elettronico e non li elaborano o trasmettono in loco. Tali esercenti devono convalidare la propria conformità completando il questionario SAQ A e l'attestato di conformità ad esso associato, confermando che:*

- La società esegue solo transazioni con carta non presente (e-commerce o via posta/telefono).
- La società non memorizza, elabora o trasmette dati di titolari di carta in loco, ma si affida interamente a provider di servizi di terze parti per tali operazioni.
- La società ha confermato che il provider di servizi di terza parte che si occupa della memorizzazione, dell'elaborazione e/o della trasmissione dei dati di titolari di carta è conforme agli standard PCI DSS.
- La società conserva solo resoconti o ricevute cartacee con i dati di titolari di carta e questi documenti non sono in formato elettronico.
- La società non memorizza i dati di titolari di carta in formato elettronico.

**Questa opzione non è mai applicabile ad esercenti con un ambiente POS che prevede il contatto diretto con i clienti.**

### Conformità agli standard PCI DSS – Operazioni

1. Completare il *questionario di autovalutazione (SAQ A)* in base alle istruzioni contenute nel documento *Istruzioni e linee guida per l'autovalutazione*.
2. Completare per intero l'attestato di conformità.
3. Inviare il questionario SAQ e l'attestato di conformità, insieme ad eventuale altra documentazione richiesta, al proprio acquirente.

### Guida per la non applicabilità di determinati requisiti specifici

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

## Attestato di conformità, SAQ A

### Istruzioni per l'invio

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

### Parte 1. Informazioni su società Qualified Security Assessor (se applicabile)

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

### Parte 2. Informazioni su società esercente

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

### Parte 2a. Tipo di settore di attività dell'esercente (selezionare tutte le risposte applicabili):

- Rivenditore     
  Telecomunicazioni     
  Market e supermarket  
 Distributori di benzina     
  E-Commerce     
  Ordini via posta/telefono     
  Altro (specificare):

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

### Parte 2b. Rapporti

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

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

## Parte 2c. Idoneità per il completamento del questionario SAQ A

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

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | L'esercente non memorizza, elabora o trasmette dati di titolari di carta in loco, ma si affida interamente a provider di servizi di terze parti per tali operazioni.               |
| <input type="checkbox"/> | Il provider di servizi di terze parti che si occupa della memorizzazione, dell'elaborazione e/o della trasmissione dei dati di titolari di carta è conforme agli standard PCI DSS. |
| <input type="checkbox"/> | L'esercente non memorizza dati di titolari di carta in formato elettronico.  |
| <input type="checkbox"/> | L'esercente conserva i dati di titolari di carta solo in forma di resoconti o copie di ricevute cartacee e non in formato elettronico.   |

## Parte 3. Convalida PCI DSS

In base ai risultati del questionario SAQ A datato (*completion date*), (*Merchant Company Name*) dichiara il seguente stato di conformità (selezionare una risposta):

- Conforme:** tutte le sezioni del questionario SAQ PCI sono state completate e a tutte le domande è stato risposto "sì", determinando una valutazione di **CONFORMITÀ** globale; pertanto (*Merchant Company Name*) ha dimostrato la massima conformità agli standard PCI DSS.
- Non conforme:** non tutte le sezioni del questionario SAQ PCI sono state completate e ad alcune domande è stato risposto "no", determinando una valutazione di **NON CONFORMITÀ** globale; pertanto (*Merchant Company Name*) non ha dimostrato la massima conformità agli standard PCI DSS.
- **Data di scadenza** per conformità:
  - È possibile che a un'entità che invia questo modulo con lo stato 'Non conforme' venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. *Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

## Parte 3a. Conferma dello stato di conformità

L'esercente conferma che:

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | Il questionario di autovalutazione A PCI DSS, versione ( <i>SAQ version #</i> ), è stato completato in base alle istruzioni qui fornite.   |
| <input type="checkbox"/> | Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione. |
| <input type="checkbox"/> | Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard.   |

## Parte 3b. Accettazione da parte dell'esercente

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

*Società esercente rappresentata* ↑

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

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

| Requisito PCI DSS | Descrizione del requisito   | Stato di conformità (selezionare una risposta) |                          | Data e azioni di correzione (in caso di non conformità) |
|-------------------|---|--|--------------------------|---|
|                   |   | SÌ   | NO                       |   |
| 9                 | Limitare l'accesso fisico ai dati di titolari di carta              | <input type="checkbox"/>                       | <input type="checkbox"/> |   |
| 12                | Gestire una politica che garantisca la sicurezza delle informazioni | <input type="checkbox"/>                       | <input type="checkbox"/> |   |

## Questionario di autovalutazione A

Data di completamento:

### Implementazione di rigide misure di controllo dell'accesso

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

| Domanda |  | Risposta: | <u>Si</u>                | <u>No</u>                | <u>Speciale*</u> |
|---------|--|-----------|--------------------------|--------------------------|------------------|
| 9.6     | Tutti i supporti cartacei ed elettronici contenenti i dati dei titolari di carta sono conservati in un luogo fisicamente sicuro?   |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9.7     | (a) La distribuzione interna ed esterna di qualsiasi tipo di supporto contenente dati di titolari di carta è rigorosamente controllata?  |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
|         | (b) I controlli devono includere quanto segue:   |           |                          |                          |                  |
| 9.7.1   | Il supporto è classificato in modo che possa essere identificato come contenente dati riservati?   |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9.7.2   | Il supporto è stato inviato tramite un corriere affidabile o un altro metodo di consegna che può essere monitorato in modo appropriato?  |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9.8     | Sono in atto processi e procedure per garantire che il management abbia dato l'approvazione prima di spostare qualsiasi supporto contenente dati di titolari da un'area protetta (in particolare quando i supporti vengono distribuiti a singole persone)? |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9.9     | Sono in atto controlli adeguati per la memorizzazione e l'accesso a supporti contenenti dati di titolari di carta?   |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9.10    | I supporti contenenti dati di titolari di carta vengono distrutti quando non sono più necessari per scopi aziendali o legali?<br>I supporti devono essere eliminati in uno dei seguenti modi:  |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9.10.1  | I materiali cartacei sono stati distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo che non sia possibile ricostruirli?   |           | <input type="checkbox"/> | <input type="checkbox"/> |                  |

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

## Gestire una politica di sicurezza delle informazioni

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

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

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

## **Appendice A: (non utilizzata)**

*Questa pagina è stata lasciata intenzionalmente vuota.*

## Appendice B: Controlli compensativi

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

I controlli compensativi devono soddisfare i seguenti criteri:

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

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

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

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

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

## Appendice C: Foglio di lavoro - Controlli compensativi

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

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

### Numero e definizione del requisito:

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

## Foglio di lavoro Controlli compensativi - Esempio

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

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

|   | Informazioni richieste   | Spiegazione   |
|---|--|---|
| <b>1. Vincoli</b>                               | 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>   |
| <b>2. Obiettivo</b>                             | 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>   |
| <b>3. Rischio identificato</b>                  | 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>   |
| <b>4. Definizione di controlli compensativi</b> | 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> |
| <b>7. Convalida dei controlli compensativi</b>  | 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>   |
| <b>8. Manutenzione</b>                          | 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>  |

