



**Payment Card Industry (PCI)
Data Security Standard
Questionario di autovalutazione**

Istruzioni e linee guida

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

Modifiche del documento	ii
Informazioni sul documento	1
Autovalutazione degli standard PCI DSS: Compatibilità	2
PCI DSS: Documenti correlati	3
Panoramica del questionario di autovalutazione (SAQ)	4
Perché è importante la conformità agli standard PCI DSS?.....	5
Suggerimenti generali e strategie per prepararsi per la convalida della conformità.....	6
Scelta del questionario e dell'attestato più appropriati per la propria azienda.....	8
<i>Tipo di convalida SAQ 1 / SAQ A: Carta non presente, tutte le funzioni per i dati di titolari di carta sono fornite dall'esterno.....</i>	<i>8</i>
<i>Tipo di convalida SAQ 2 / SAQ B: Esercenti che utilizzano solo macchinetta stampigliatrice, nessuna memorizzazione dei dati di titolari di carta</i>	<i>9</i>
<i>Tipo di convalida SAQ 3 / SAQ B: Esercenti che utilizzano solo terminali per connessione in uscita indipendenti, nessuna memorizzazione elettronica dei dati di titolari di carta.....</i>	<i>9</i>
<i>Tipo di convalida SAQ 4 / SAQ C: Esercenti con sistemi di pagamento connessi a Internet</i>	<i>9</i>
<i>Tipo di convalida SAQ 5 / SAQ D: Tutti gli altri esercenti e provider di servizi definiti da un marchio di pagamento come idonei per completare un questionario SAQ.....</i>	<i>10</i>
<i>Guida per l'esclusione e la non applicabilità di determinati requisiti specifici.....</i>	<i>10</i>
Istruzioni per il completamento del questionario SAQ	11
Istruzioni e linee guida per l'autovalutazione — Qual è il mio tipo di convalida?	12

Informazioni sul documento

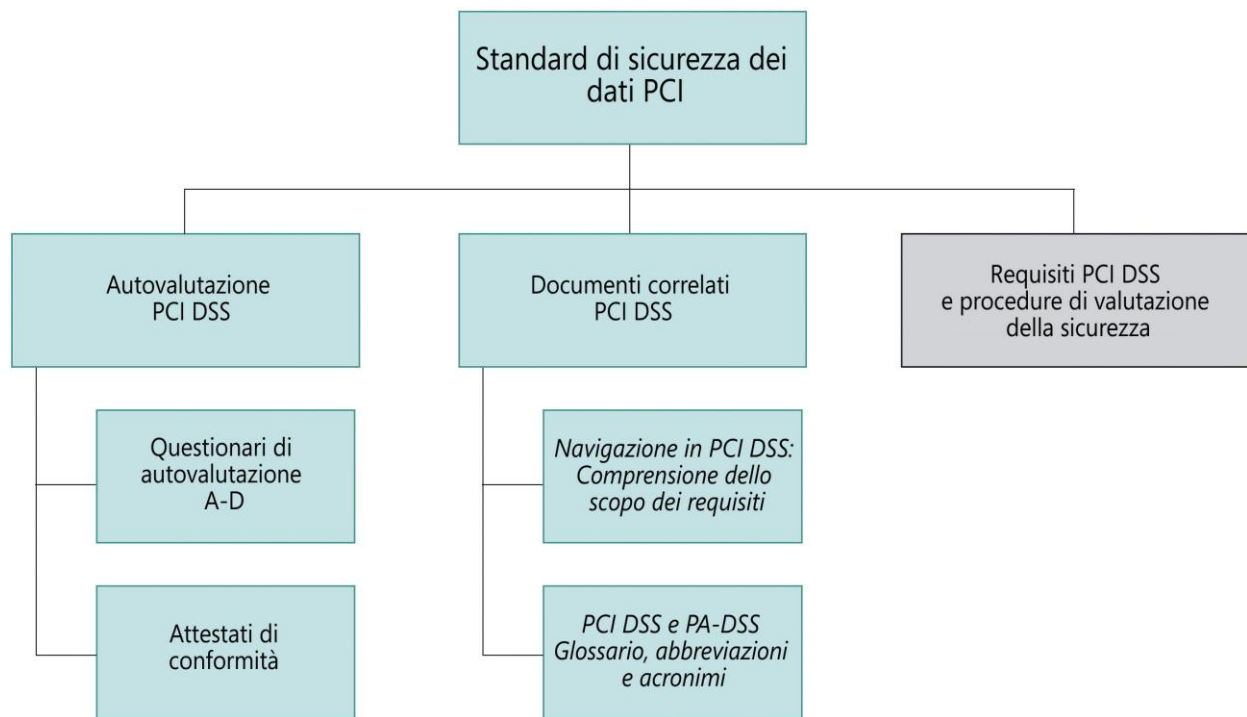
Questo documento è stato sviluppato per aiutare gli esercenti e i provider di servizi a comprendere il questionario di autovalutazione (SAQ, Self-Assessment Questionnaire) degli standard di sicurezza (DSS, Data Security Standard) PCI. Leggere completamente il documento per comprendere il motivo per cui gli standard PCI DSS sono importanti per la propria azienda, le possibili strategie da utilizzare per facilitare la convalida della conformità e determinare se la propria azienda dispone dei requisiti necessari per completare una delle versioni del questionario più brevi. Nelle sezioni seguenti vengono fornite tutte le informazioni necessarie sul questionario di autovalutazione PCI DSS.

- Autovalutazione degli standard PCI DSS: Compatibilità
- PCI DSS: Documenti correlati
- Panoramica del questionario di autovalutazione (SAQ)
- Perché è importante la conformità agli standard PCI DSS?
- Suggerimenti generali e strategie
- Scelta del questionario più appropriato per la propria azienda
- Guida per l'esclusione e la non applicabilità di determinati requisiti specifici
- Completamento del questionario

Autovalutazione degli standard PCI DSS: Compatibilità

Gli standard di sicurezza dei dati PCI e i documenti correlati rappresentano una serie comune di strumenti e misurazioni del settore che consentono di gestire in modo più sicuro le informazioni riservate. Gli standard forniscono una struttura azionabile per lo sviluppo di un processo per la protezione dei dati dei clienti affidabile, che comprende la prevenzione, il rilevamento e la risposta a problemi di sicurezza. Per limitare il rischio di violazioni della sicurezza e ridurre l'impatto, è importante che tutte le entità che memorizzano, elaborano o trasmettono dati di titolari di carta agiscano nel rispetto di tali standard. Il grafico seguente mostra gli strumenti che aiutano le diverse entità interessate a garantire la conformità agli standard di sicurezza dei dati PCI e ad eseguire la relativa autovalutazione.

Questi e altri documenti correlati sono disponibili all'indirizzo www.pcisecuritystandards.org.



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 ¹
<i>PCI DSS: Questionario di autovalutazione B e Attestato</i>	Esercenti ¹
<i>PCI DSS: Questionario di autovalutazione C e Attestato</i>	Esercenti ¹
<i>PCI DSS: Questionario di autovalutazione D e Attestato</i>	Gli esercenti ¹ e tutti i provider di servizi
<i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>	Tutti gli esercenti e i provider di servizi

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

Panoramica del questionario di autovalutazione (SAQ)

Il questionario di autovalutazione della conformità agli standard di sicurezza dei dati PCI è uno strumento di convalida che assiste esercenti e provider di servizi nell'autovalutazione della propria conformità agli standard di sicurezza dei dati delle carte di pagamento (PCI DSS). Per soddisfare diversi scenari, sono disponibili tre versioni del questionario di autovalutazione PCI DSS. Questo documento è stato sviluppato per aiutare le aziende a scegliere il questionario più appropriato alle loro esigenze.

Il questionario di autovalutazione PCI DSS è uno strumento di convalida per esercenti e provider di servizi non richiesto per una valutazione della sicurezza dei dati in loco in base al documento Requisiti PCI DSS e procedure di valutazione della sicurezza, ma può essere richiesto dal proprio acquirente o marchio di pagamento. Consultare l'acquirente o il marchio di pagamento per informazioni dettagliate sui requisiti di convalida PCI DSS.

Il questionario di autovalutazione degli standard PCI DSS è costituito dai seguenti componenti:

1. Domande correlate ai requisiti PCI DSS, appropriate per provider di servizi ed esercenti: vedere la sezione "Scelta del questionario SAQ e dell'attestato più appropriati per la propria azienda" nel presente documento.
2. Attestato di conformità: l'attestato è la certificazione della propria idoneità per eseguire e aver eseguito l'autovalutazione appropriata.

Perché è importante la conformità agli standard PCI DSS?

I membri del PCI Security Standards Council (American Express, Discover, JCB, MasterCard e Visa) controllano continuamente casi di compromissione dei dati dei clienti. Questi casi riguardano l'intera gamma di aziende, da aziende di piccole dimensioni a esercenti e provider di servizi molto grandi.

Una violazione della sicurezza e la successiva compromissione dei dati della carta di pagamento hanno effetti di vasta portata sulle entità interessate, tra cui:

1. Obbligo di notifica alle autorità regolatorie
2. Danni alla reputazione
3. Perdita di clienti
4. Possibili responsabilità finanziarie (ad esempio, sanzioni regolatorie e altre sanzioni e multe)
5. Cause legali

L'analisi post-mortem dei danni ha mostrato i punti deboli comuni in termini di sicurezza che sono risolti dagli standard di sicurezza dei dati PCI, ma che non erano stati presi in considerazione nelle aziende in cui si sono verificati tali problemi. Gli standard PCI DSS includono requisiti dettagliati esattamente per questo motivo, ossia per ridurre al minimo la possibilità di compromettere la sicurezza dei dati e i conseguenti effetti.

In base ad alcune indagini eseguite successivamente, sono state rilevate alcune violazioni degli standard PCI DSS comuni, incluse senza limitazione:

- Memorizzazione di dati della striscia magnetica (requisito 3.2). È importante tenere presente che molte entità danneggiate non sono a conoscenza del fatto che i relativi sistemi memorizzino questi dati.
- Controlli dell'accesso inadeguati dovuti a sistemi POS per esercenti installati in modo non corretto, che consentono agli hacker di accedere ad aree destinate ai fornitori di POS (requisiti 7.1, 7.2, 8.2 e 8.3)
- Impostazioni di sistema e password predefinite non modificate dal momento della configurazione del sistema (requisito 2.1)
- Servizi non necessari e non protetti non rimossi o modificati dal momento della configurazione del sistema (requisito 2.2.2)
- Applicazioni Web codificate in modo scadente che portano a problemi di SQL Injection e altre vulnerabilità e consentono di accedere al database contenente i dati dei titolari di carta di direttamente dal sito Web (requisito 6.5)
- Patch di sicurezza mancanti e obsolete (requisito 6.1)
- Perdita dei log (requisito 10)
- Mancanza di meccanismi di monitoraggio (mediante revisioni di log, rilevazione/prevenzione delle intrusioni, analisi delle vulnerabilità trimestrali e sistemi di monitoraggio dell'integrità dei file) (requisiti 10.6, 11.2, 11.4 e 11.5)
- Perdita di segmentazione in una rete, rendendo facilmente accessibili i dati di titolari di carta attraverso punti deboli di altre parti della rete (ad esempio, da punti accesso wireless, posta elettronica dei dipendenti ed esplorazione Web) (requisiti 1.3 e 1.4)

Suggerimenti generali e strategie per prepararsi per la convalida della conformità

Di seguito alcuni suggerimenti generali e alcune strategie per convalidare la propria conformità agli standard PCI DSS. Questi suggerimenti possono aiutare a eliminare i dati non necessari, isolare i dati **necessari** in aree centralizzate definite e controllate e limitare l'ambito della convalida della conformità agli standard PCI DSS. Ad esempio, eliminando i dati non necessari e/o isolando tali dati in aree definite e controllate, è possibile eliminare dall'autovalutazione sistemi e reti non più utilizzati per memorizzare, elaborare o trasmettere i dati dei titolari di carta.

1. Dati sensibili di autenticazione (includono il contenuto completo della striscia magnetica, i codici e i valori di validazione della carta e i blocchi PIN):

- a. Accertarsi di **non memorizzare mai questi dati**.
- b. In caso di dubbio, contattare il fornitore del sistema POS per verificare se il prodotto e la versione software in uso memorizza tali dati. In alternativa, considerare l'assunzione di un Qualified Security Assessor (QSA) in grado di fornire il supporto necessario per determinare se dati sensibili di autenticazione sono memorizzati, registrati o acquisiti dal sistema in uso.

2. In qualità di esercente, chiedere al fornitore del sistema POS informazioni sulla sicurezza del sistema in uso, ponendo le seguenti domande consigliate:

- a. Il mio software POS è convalidato in base agli standard PA-DSS (fare riferimento all'elenco PCI SSC di applicazioni di pagamento convalidate)?
- b. Il mio software POS memorizza dati della striscia magnetica (dati su traccia) o blocchi PIN? In tal caso, poiché questa memorizzazione è vietata, può aiutarmi a eliminare tali dati nel tempo più breve possibile?
- c. È in atto un processo per creare un elenco dei file scritti dall'applicazione con un riepilogo del contenuto di ciascun file che consenta di verificare che tali dati di cui è vietata la conservazione non siano realmente memorizzati?
- d. Il sistema POS richiede l'installazione di firewall per proteggere il mio sistema da un accesso non autorizzato?
- e. Sono necessarie password complesse e univoche per accedere ai miei sistemi? Può confermare che non vengono utilizzate password comuni o predefinite per accedere al mio sistema e ai sistemi di altri esercenti suoi clienti?
- f. Le impostazioni e le password predefinite sono state modificate nei sistemi e nei database che fanno parte del sistema POS?
- g. Tutti i servizi non necessari e non sicuri sono stati rimossi dai sistemi e dai database che fanno parte del sistema POS?
- h. Può accedere in remoto al mio sistema POS? In tal caso, ha implementato controlli appropriati per impedire ad altre persone di accedere al mio sistema POS, ad esempio metodi di accesso remoto sicuri e non tramite password comuni o predefinite? Con quale frequenza accede al mio sistema POS in remoto e perché? Chi è autorizzato ad accedere al mio sistema POS in remoto?
- i. Tutti i sistemi e i database che fanno parte del sistema POS sono stati aggiornati con tutte le patch di sicurezza applicabili?
- j. La funzionalità di creazione di file di log è attivata per i sistemi e i database che fanno parte del sistema POS?
- k. Se le versioni precedenti del mio software POS prevedevano la memorizzazione dei dati su traccia, questa funzione è stata rimossa dalla versione corrente del software POS? È stata utilizzata una funzionalità per la pulizia del sistema sicura per rimuovere questi dati?

3. Dati di titolari di carta — Se non sono necessari, non conservarli!

- a. Le regole dei marchi di pagamento consentono la memorizzazione del numero PAN (Personal Account Number, numero account personale), della data di scadenza, del nome del titolare e del codice di servizio.
- b. Fare un inventario di tutti i motivi e i luoghi in cui si conservano questi dati. Se i dati non sono più necessari per uno scopo aziendale significativo, considerarne l'eliminazione.
- c. Determinare se la conservazione di tali dati e il processo aziendale basato su tale conservazione giustificano i seguenti rischi:
 - i. Compromissione dei dati
 - ii. Necessità di ulteriori azioni per proteggere tali dati nel rispetto degli standard PCI DSS
 - iii. Necessità di azioni di manutenzione continue per rimanere conformi agli standard PCI DSS nel tempo

4. Dati di titolari di carta — Se sono necessari, consolidarli e isolarli.

- a. È possibile limitare l'ambito di una valutazione della conformità agli standard PCI DSS conservando i dati in un ambiente specifico e isolando tali dati mediante l'uso di una segmentazione di rete appropriata. Ad esempio, se i dipendenti navigano in Internet e ricevono un messaggio e-mail sullo stesso computer o sullo stesso segmento di rete utilizzato per i dati di titolari di carta, considerare la segmentazione (isolamento) di tali dati in un computer o in un segmento di rete specifico (mediante router o firewall). Un isolamento efficiente dei dati di titolari di carta consente di concentrare i propri sforzi per garantire la conformità agli standard PCI DSS solo sulla parte isolata anziché su tutti i computer.

5. Controlli compensativi

- a. È possibile considerare controlli compensativi per la maggior parte dei requisiti PCI DSS quando un'entità non è in grado di soddisfare le specifiche tecniche di un requisito, ma ha posto in essere altri controlli sufficienti a mitigare il rischio associato a tale requisito. Se la propria società non esegue il controllo esatto specificato negli standard PCI DSS, ma ha messo in atto altri controlli che soddisfano la definizione PCI DSS di controlli compensativi (vedere "Controlli compensativi" nell'appendice del questionario SAQ applicabile e il documento *PCI DSS Glossario, abbreviazioni e acronimi* www.pcisecuritystandards.org), la società deve effettuare quanto segue:
 - i. Rispondere "Sì" alla domanda del questionario SAQ e, nella colonna "Speciale", annotare l'uso di ciascun controllo compensativo utilizzato per soddisfare un requisito.
 - ii. Rivedere la sezione "Controlli compensativi" nell'appendice e documentare l'uso di tali controlli completando il corrispondente foglio di lavoro.
 - a) Completare un foglio di lavoro dei controlli compensativi per ciascun requisito soddisfatto con un controllo di questo tipo.
 - iii. Inviare tutti i fogli di lavoro dei controlli compensativi, insieme al questionario completato e/o all'attestato, in base alle istruzioni dell'acquirente o del marchio di pagamento.

6. Assistenza professionale

- a. Se si desidera ricevere istruzioni e linee guida da un professionista della sicurezza per garantire la conformità e completare il questionario SAQ, non esitare. Considerare, tuttavia, che, sebbene sia possibile scegliere qualsiasi professionista della sicurezza si desideri, solo i professionisti inclusi nell'elenco di Qualified Security Assessor (QSA) di PCI SSC sono riconosciuti come QSA e formati da PCI SSC. Questo elenco è disponibile all'indirizzo https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Scelta del questionario e dell'attestato più appropriati per la propria azienda

In base alle regole del marchio di pagamento, tutti gli esercenti e i provider di servizi devono garantire la conformità a tutti gli standard di sicurezza dei dati PCI. Esistono cinque categorie di convalida SAQ, mostrate brevemente nella tabella seguente e descritte più dettagliatamente nei seguenti paragrafi. Utilizzare la tabella per valutare quale questionario SAQ è più appropriato per la propria azienda ed esaminare le descrizioni dettagliate per accertarsi di soddisfare tutti i requisiti previsti nel questionario scelto.

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

Tipo di convalida SAQ 1 / SAQ A: Carta non presente, tutte le funzioni per i dati di titolari di carta sono fornite dall'esterno

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 che appartengono al tipo di convalida 1 non memorizzano i dati di titolari di carta in formato elettronico e non elaborano o trasmettono tali dati in loco; 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 terze parti per tali operazioni.
- La società ha confermato che la 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.

Per una guida grafica per la scelta del tipo di convalida, vedere "Istruzioni e linee guida per l'autovalutazione — Qual è il mio tipo di convalida" a pagina 12.

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

Tipo di convalida SAQ 2 / SAQ B: Esercenti che utilizzano solo macchinetta stampigliatrice, nessuna memorizzazione dei dati di titolari di carta

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

Gli esercenti del tipo di convalida 2 elaborano i dati di titolari di carta solo tramite macchinette stampigliatrici e devono convalidare la propria conformità completando il questionario SAQ B e l'attestato di conformità ad esso associato, confermando che:

- La società utilizza solo una macchinetta stampigliatrice per acquisire i dati della carta di pagamento dei clienti.
- La società non trasmette i dati di titolari di carta telefonicamente o tramite Internet.
- La società conserva solo copie cartacee delle ricevute.
- La società non memorizza i dati di titolari di carta in formato elettronico.

Per una guida grafica per la scelta del tipo di convalida, vedere "Istruzioni e linee guida per l'autovalutazione — Qual è il mio tipo di convalida" a pagina 12.

Tipo di convalida SAQ 3 / SAQ B: Esercenti che utilizzano solo terminali per connessione in uscita indipendenti, nessuna memorizzazione elettronica dei dati di titolari di carta

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

Gli esercenti che appartengono al tipo di convalida 3 elaborano i dati di titolari di carta mediante terminali per connessione in uscita indipendenti e possono essere società di e-commerce con punti vendita reali (carta presente) o società di e-commerce o vendita tramite posta elettronica/telefono (carta non presente). Gli esercenti del tipo di convalida 3 garantiscono la propria conformità completando il questionario SAQ B e l'attestato di conformità ad esso associato, confermando che:

- La società utilizza solo terminali per la connessione in uscita indipendenti (connessi tramite la linea telefonica al processore).
- I terminali per connessione in uscita indipendenti non sono connessi ad altri sistemi all'interno dell'ambiente.
- I terminali per connessione in uscita indipendenti non sono connessi a Internet.
- La società conserva solo resoconti o copie cartacee delle ricevute.
- La società non memorizza i dati di titolari di carta in formato elettronico.

Tipo di convalida SAQ 4 / SAQ C: Esercenti con sistemi di pagamento connessi a Internet

Il questionario SAQ C è stato sviluppato per rispondere ai requisiti applicabili ad esercenti i cui sistemi di pagamento (ad esempio, punto di vendita con sistemi di shopping online) sono connessi a Internet (tramite connessione ad alta velocità, DSL, modem via cavo, ecc.) per uno dei due seguenti motivi:

1. Il sistema di pagamento si trova su un computer connesso a Internet (ad esempio, per operazioni e-mail o Web).
2. Il sistema di pagamento è connesso a Internet per trasmettere i dati di titolari di carta.

Gli esercenti che appartengono al tipo di convalida 4 elaborano i dati di titolari di carta mediante sistemi di pagamento connessi a Internet, non memorizzano tali dati su un computer e possono essere società di e-commerce con punti vendita reali (carta presente) o società di e-commerce o vendita tramite posta elettronica/telefono (carta non presente). Gli esercenti del tipo di convalida 4 devono garantire la propria conformità completando il questionario SAQ C e l'attestato di conformità ad esso associato, confermando che:

- La società ha un sistema di pagamento e una connessione Internet sullo stesso computer.
- Il dispositivo con il sistema di pagamento/Internet non è connesso ad altri sistemi all'interno del proprio ambiente.
- La società conserva solo resoconti o copie cartacee delle ricevute.
- La società non memorizza i dati di titolari di carta in formato elettronico.
- Il fornitore del software del sistema di pagamento della società utilizza tecniche sicure per fornire supporto in remoto al sistema di pagamento.

Per una guida grafica per la scelta del tipo di convalida, vedere "Istruzioni e linee guida per l'autovalutazione — Qual è il mio tipo di convalida" a pagina 12.

Tipo di convalida SAQ 5 / SAQ D: Tutti gli altri esercenti e provider di servizi definiti da un marchio di pagamento come idonei per completare un questionario SAQ

Il questionario SAQ D è stato sviluppato per rispondere ai requisiti applicabili a tutti i provider di servizi definiti da un marchio di pagamento come idonei per completare un questionario SAQ e a tutti gli esercenti che non rientrano nei tipi di convalida da 1 a 4, sopra descritti.

I provider di servizi e gli esercenti del tipo di convalida 5 devono convalidare 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 non può garantire la conformità ai requisiti indicati nelle sezioni degli standard PCI DSS specifiche di tale tecnologia. Fare riferimento alla guida seguente per informazioni sull'esclusione dei requisiti relativi alla tecnologia wireless e di determinati altri requisiti specifici.

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

Esclusione: Se per convalidare la propria conformità agli standard PCI DSS occorre completare il questionario SAQ C o D, è possibile considerare le seguenti eccezioni: Vedere "Non applicabilità" di seguito per la risposta appropriata al questionario SAQ.

- Requisiti 1.2.3 (SAQ D), 2.1.1 (SAQ C e D) e 4.1.1 (SAQ D): Fornire una risposta a queste domande specifiche della tecnologia wireless solo se tale tecnologia è disponibile nella propria rete. Tenere presente che occorre comunque fornire una risposta al requisito 11.1 (uso di analizzatore wireless) anche se la propria rete non prevede la tecnologia wireless, perché l'analizzatore rileva eventuali intrusioni o dispositivi non autorizzati che possono essere stati aggiunti a vostra insaputa.
- Requisiti 6.3-6.5 (SAQ D): Fornire una risposta a queste domande specifiche di applicazioni e codice personalizzati solo se la propria azienda sviluppa applicazioni Web personalizzate.
- Requisiti 9,1-9,4 (SAQ D): Fornire una risposta a queste domande solo per strutture con "aree sensibili" come definite nel presente documento. Per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.

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

Istruzioni per il completamento del questionario SAQ

1. Utilizzare le presenti linee guida per determinare il questionario SAQ appropriato per la propria azienda.
2. Utilizzare il documento *Navigazione in PCI DSS: Comprensione dello scopo dei requisiti* per comprendere come e perché i requisiti sono rilevanti per la propria azienda.
3. Utilizzare il questionario SAQ appropriato come strumento per convalidare la conformità agli standard PCI DSS.
4. Seguire le istruzioni disponibili nella sezione Conformità agli standard PCI DSS - Operazioni del questionario SAQ appropriato e fornire tutta la documentazione richiesta al proprio acquirente o marchio di pagamento, come necessario.

Istruzioni e linee guida per l'autovalutazione — Qual è il mio tipo di convalida?

