

**Settore delle carte di pagamento (PCI)
Standard di protezione dei dati
Questionario di autovalutazione A
e Attestato di conformità**

**Esercenti carta non presente,
tutte le funzioni per i dati dei titolari di carta sono
fornite dall'esterno**

Per l'uso con PCI DSS versione 3.2

Aprile 2016

Modifiche del documento

Data	Versione PCI DSS	Revision e SAQ	Descrizione
Ottobre 2008	1.2		Allineare il contenuto con il nuovo standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.
Ottobre 2010	2.0		Allineare il contenuto ai nuovi requisiti e procedure di test PCI DSS v2.0.
Febbraio 2014	3.0		Allineare il contenuto con i requisiti PCI DSS v3.0 e le procedure di test e incorporare ulteriori opzioni di risposta.
Aprile 2015	3.1		Aggiornato per allinearli a PCI DSS v3.1. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.0 alla 3.1</i> .
Luglio 2015	3.1	1.1	Numerazione delle versioni aggiornata per allinearla ad altri questionari SAQ.
Aprile 2016	3.2	1.0	Aggiornato per allinearli a PCI DSS v3.2. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.1 alla 3.2</i> .

Sommario

Modifiche del documento	i
Operazioni preliminari	iii
Passaggi per il completamento dell'autovalutazione PCI DSS	iii
Comprensione del questionario di autovalutazione	iv
<i>Test previsti</i>	<i>iv</i>
Completamento del questionario di autovalutazione	v
Guida per la non applicabilità di determinati requisiti specifici	v
Eccezione legale	v
Sezione 1 - Informazioni sulla valutazione	1
Sezione 2 - Questionario di autovalutazione A	4
Sviluppo e gestione di sistemi e reti sicure	4
<i>Requisito 2 - Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione</i>	<i>4</i>
Implementazione di rigide misure di controllo dell'accesso	5
<i>Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema</i>	<i>5</i>
<i>Requisito 9 - Limitare l'accesso fisico ai dati dei titolari di carta</i>	<i>6</i>
Gestire una politica di sicurezza delle informazioni	7
<i>Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale</i>	<i>8</i>
Appendice A - Requisiti PCI DSS aggiuntivi	10
<i>Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i>	<i>10</i>
<i>Appendice A2 - Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale</i>	<i>10</i>
<i>Appendice A3 - Convalida aggiuntiva delle entità designate (DESV)</i>	<i>10</i>
Appendice B - Foglio di lavoro - Controlli compensativi	11
Appendice C - Spiegazione di non applicabilità	12
Sezione 3 - Dettagli su convalida e attestato	13

Operazioni preliminari

Il modulo SAQ A è stato sviluppato per rispondere ai requisiti applicabili agli esercenti le cui funzioni per i dati dei titolari di carta sono state completamente esternalizzate a terzi convalidati, per cui l'esercente conserva soltanto i resoconti cartacei o le ricevute con i dati dei titolari di carta.

Gli esercenti SAQ A possono svolgere la propria attività sia mediante e-commerce che ordini per posta/telefono (con carta non presente) e non memorizzano, elaborano o trasmettono i dati dei titolari di carta in formato elettronico nei loro sistemi o presso le loro sedi.

Gli esercenti SAQ A confermano che, per questo canale di pagamento:

- La società accetta solo transazioni con carta non presente (e-commerce o via posta/telefono).
- Tutte le operazioni di elaborazione dei dati dei titolari di carta vengono interamente esternalizzate a provider di servizi di terzi convalidati PCI DSS.
- La società non memorizza, elabora o trasmette in formato elettronico i dati di titolari di carta nei sistemi o in sede, ma si affida interamente a provider di servizi di terze parti per tutte queste 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 eventuali dati dei titolari di carta su carta (ad esempio, resoconti o ricevute cartacei) e questi documenti non sono in formato elettronico.

Inoltre, per canali di e-commerce:

- Tutti gli elementi delle pagine di pagamento che vengono inviati al browser del consumatore provengono solo e direttamente da un provider di servizi di terzi PCI DSS convalidato.

Questo SAQ non è applicabile ai canali che prevedono un contatto diretto con il cliente.

Questa versione più breve del questionario di autovalutazione comprende domande che riguardano un tipo specifico di ambiente di esercenti di dimensioni ridotte, secondo quanto definito nei criteri di idoneità esposti in precedenza. Qualora siano presenti requisiti PCI DSS applicabili al proprio ambiente che non sono coperti dal presente questionario di autovalutazione, ciò potrebbe indicare che questo questionario non è adatto al proprio ambiente. Inoltre, è comunque necessario soddisfare tutti i requisiti PCI DSS applicabili per garantire la conformità agli standard PCI DSS.

Passaggi per il completamento dell'autovalutazione PCI DSS

1. Identificare il questionario SAQ per il proprio ambiente. Per informazioni, consultare il documento *Istruzioni e linee guida per l'autovalutazione* sul sito Web PCI SSC.
2. Accertarsi che il proprio ambiente sia del giusto ambito e che risponda ai criteri di idoneità per il questionario SAQ che si sta utilizzando (come definito alla sezione 2g dell'Attestato di conformità).
3. Valutare il proprio ambiente per la conformità ai requisiti PCI DSS applicabili.
4. Completare tutte le sezioni di questo documento:
 - Sezione 1 (Parti 1 e 2 dell'AOC) - Informazioni sulla valutazione e riepilogo esecutivo
 - Sezione 2 - Questionario di autovalutazione PCI DSS (SAQ A)
 - Sezione 3 (Parti 3 e 4 dell'AOC) - Dettagli su convalida e attestato e piano d'azione per i requisiti non conformi (se applicabile)
5. Inviare il questionario SAQ e l'Attestato di conformità (AOC), insieme ad eventuale altra documentazione richiesta (ad esempio, i rapporti delle scansioni ASV) al proprio acquirente, al marchio di pagamento o ad altra entità richiedente.

Comprensione del questionario di autovalutazione

Le domande contenute nella colonna “Domanda PCI DSS” del presente questionario di autovalutazione si basano sui requisiti specificati negli standard PCI DSS.

Sono inoltre state fornite risorse aggiuntive a supporto del processo di valutazione che forniscono indicazioni sui requisiti PCI DSS e sulla procedura di compilazione del questionario di autovalutazione. Di seguito è disponibile una panoramica di alcune di queste risorse:

Documento	Include:
PCI DSS <i>(Requisiti PCI DSS e procedure di valutazione della sicurezza)</i>	<ul style="list-style-type: none"> • Istruzioni sulla determinazione dell’ambito • Istruzioni sullo scopo di tutti i requisiti PCI DSS • Dettagli delle procedure di test • Istruzioni sui controlli compensativi
Documenti relativi a istruzioni e linee guida SAQ	<ul style="list-style-type: none"> • Informazioni su tutti i questionari SAQ e sui relativi criteri di idoneità • Come determinare quale questionario SAQ è adatto alla propria azienda
<i>Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS</i>	<ul style="list-style-type: none"> • Descrizioni e definizioni dei termini utilizzati in PCI DSS e nei questionari di autovalutazione

Queste e altre risorse sono disponibili sul sito Web PCI SSC (www.pcisecuritystandards.org). Le aziende sono invitate a esaminare gli standard PCI DSS e altri documenti di supporto prima di iniziare una valutazione.

Test previsti

Le istruzioni fornite nella colonna “Test previsti” si basano sulle procedure di test contenute negli standard PCI DSS e forniscono una descrizione dettagliata dei tipi di attività di test che devono essere eseguiti al fine di verificare la conformità a un requisito. I dettagli completi delle procedure di test per ogni requisito sono disponibili negli standard PCI DSS.

Completamento del questionario di autovalutazione

Per ogni domanda vengono fornite diverse risposte tra cui scegliere per indicare lo stato della propria azienda in merito al requisito specificato. **È possibile selezionare una sola risposta per ogni domanda.**

Nella tabella riportata di seguito viene fornita una descrizione del significato di ogni risposta:

Risposta	Quando utilizzare questa risposta:
Sì	Il test previsto è stato eseguito e tutti gli elementi del requisito sono stati soddisfatti come indicato.
Sì con CCW (Foglio di lavoro - Controllo compensativo)	<p>Il test previsto è stato eseguito e il requisito risulta soddisfatto grazie all'ausilio di un controllo compensativo.</p> <p>Tutte le risposte di questa colonna richiedono il completamento di un Foglio di lavoro - Controllo compensativo (CCW) presente nell'Appendice B del questionario SAQ.</p> <p>Negli standard PCI DSS vengono fornite tutte le informazioni sull'utilizzo dei controlli compensativi e le istruzioni sulla procedura di completamento del foglio di lavoro.</p>
No	Alcuni o tutti gli elementi del requisito non sono stati soddisfatti, sono in fase di implementazione o richiedono ulteriori test prima di sapere se sono effettivamente in uso.
N/A (non applicabile)	<p>Il requisito non si applica all'ambiente dell'azienda. (Per consultare alcuni esempi, vedere la <i>Guida per la non applicabilità di determinati requisiti specifici</i> riportata di seguito.)</p> <p>Tutte le risposte di questa colonna richiedono una spiegazione di supporto disponibile nell'Appendice C del questionario SAQ.</p>

Guida per la non applicabilità di determinati requisiti specifici

Se si ritiene che alcuni requisiti non siano applicabili nel proprio ambiente, selezionare l'opzione "N/A" per il requisito in questione e completare il foglio di lavoro "Spiegazione di non applicabilità" presente nell'Appendice C per ogni voce "N/A".

Eccezione legale

Se la propria azienda è soggetta a una restrizione di natura legale che le impedisce di soddisfare un requisito PCI DSS, selezionare la colonna "No" specifica di quel requisito e completare l'attestato corrispondente nella Parte 3.

Sezione 1 - Informazioni sulla valutazione

Istruzioni per l'invio

Il presente documento deve essere compilato come dichiarazione dei risultati dell'autovalutazione dell'esercente unitamente a *Requisiti e procedure di valutazione della sicurezza PCI DSS*. Completare tutte le sezioni. L'esercente è tenuto a garantire che ogni sezione sia stata completata dalle parti interessate, come applicabile. Contattare l'acquirente (banca dell'esercente) o i marchi di pagamento per determinare le procedure di reporting e invio.

Parte 1. Informazioni Esercente e Azienda qualificata per la valutazione (QSA)

Parte 1a. Informazioni sull'organizzazione dell'esercente

Ragione sociale:		DBA (doing business as):	
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. Riepilogo esecutivo

Parte 2a. Tipo di esercente (selezionare tutte le risposte pertinenti)

- Rivenditore
 Telecomunicazioni
 Negozi di alimentari e supermercati
 Distributori di benzina
 E-Commerce
 Ordini via posta/telefono (MOTO)
 Altro (specificare):

Quali tipi di canali di pagamento offre l'azienda?

- Ordini via posta/telefono (MOTO)
 E-Commerce
 Con carta presente (contatto diretto)

Quali sono i canali di pagamento coperti dal presente questionario SAQ?

- Ordini via posta/telefono (MOTO)
 E-Commerce
 Con carta presente (contatto diretto)

Nota: se la propria azienda dispone di un canale o una procedura di pagamento non inclusi nel presente questionario SAQ, consultare l'acquirente o il marchio di pagamento in merito alla convalida degli altri canali.

Parte 2b. Descrizione delle attività relative alla carta di pagamento

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

Parte 2c. Sedi

Elenco dei tipi di struttura (ad esempio, punti vendita, uffici, centri dati, call center ecc.) e riepilogo delle sedi incluse nella revisione PCI DSS.

Tipo di struttura	Numero di strutture di questo tipo	Sedi della struttura (città, paese)
<i>Esempio: punti vendita</i>	3	<i>Boston, MA, Stati Uniti</i>

Parte 2d. Applicazione di pagamento

L'azienda utilizza una o più applicazioni di pagamento? Sì No

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

Nome applicazione di pagamento	Versione numero	Fornitore dell'applicazione	L'applicazione è inclusa nell'elenco PA-DSS?	Data di scadenza dell'elenco PA-DSS (se applicabile)
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	

Parte 2e. Descrizione dell'ambiente

Fornire una descrizione **di alto livello** dell'ambiente coperto da questa valutazione.

Ad esempio:

- *Connessioni interne ed esterne all'ambiente dei dati dei titolari di carta.*
- *Componenti di sistema critici interni all'ambiente dei dati dei titolari di carta, ai database, ai server Web ecc. e qualsiasi altro componente di pagamento necessario, come applicabile.*

L'azienda utilizza la segmentazione di rete per definire l'ambito del proprio ambiente PCI DSS?

Sì No

(Consultare la sezione "Segmentazione di rete" di PCI DSS per indicazioni sulla

segmentazione di rete.)

Parte 2f. Provider di servizi di terzi

L'azienda utilizza un responsabile dell'integrazione e rivenditore qualificati (QIR)?

Sì No

Se sì:

Nome dell'azienda QIR:

Singolo nome QIR:

Descrizione dei servizi forniti dal QIR:

L'azienda condivide i dati dei titolari di carta con provider di servizi di terzi (ad esempio responsabile dell'integrazione e rivenditore qualificati (QIR), gateway, elaboratori pagamenti, provider di servizi di pagamento (PSP), società di hosting Web, agenti per la prenotazione di voli aerei, agenti del programma fedeltà, ecc.)?

Sì No

Se sì:

Nome del provider di servizi:	Descrizione dei servizi forniti:

Nota: il Requisito 12.8 si applica a tutte le entità presenti in questo elenco.

Parte 2g. Idoneità al completamento del modulo SAQ A

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

- L'esercente accetta solo transazioni con carta non presente (e-commerce o via posta/telefono).
- Tutte le operazioni di elaborazione dei dati dei titolari di carta vengono interamente esternalizzate a provider di servizi di terzi convalidati PCI DSS.
- L'esercente non memorizza, elabora o trasmette dati dei titolari di carta nei propri sistemi o in sede, ma si affida interamente a provider di servizi di terzi per tali operazioni.
- L'esercente 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.
- L'esercente conserva eventuali dati dei titolari di carta su carta (ad esempio, resoconti o ricevute cartacei) e questi documenti non sono in formato elettronico.
- Inoltre, per canali di e-commerce:*
Tutti gli elementi delle pagine di pagamento che vengono inviati al browser del consumatore provengono solo e direttamente da un provider di servizi di terzi PCI DSS convalidato.

Sezione 2 - Questionario di autovalutazione A

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

Data di completamento dell'autovalutazione:

Sviluppo e gestione di sistemi e reti sicure

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Sì	Sì con CCW	No	N/A
2.1 (a) I valori predefiniti del fornitore vengono sempre modificati prima di installare un sistema in rete? <i>Questo vale per TUTTE le password predefinite, incluse, senza limitazioni, quelle utilizzate da sistemi operativi, software che fornisce servizi di sicurezza, account di applicazioni e sistemi, terminali POS (Point-Of-Sale), applicazioni di pagamento, stringhe di comunità SNMP (Simple Network Management Protocol), ecc.</i>	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Esaminare la documentazione del fornitore ▪ Osservare le configurazioni di sistema e le impostazioni account ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Gli account predefiniti non necessari vengono rimossi o disabilitati prima dell'installazione di un sistema sulla rete?	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni di sistema e le impostazioni account ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Implementazione di rigide misure di controllo dell'accesso

Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
8.1.1	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?	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	L'accesso per gli utenti non attivi viene disattivato o rimosso immediatamente?	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Esaminare gli utenti account non attivi ▪ Analizzare gli elenchi di accesso attuali ▪ Osservare i dispositivi di autenticazione fisici 	<input type="checkbox"/>	<input type="checkbox"/>	<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 un elemento biometrico. 	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Osservare i processi di autenticazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.3	(a) I parametri delle password utente vengono configurati per richiedere che password/passphrase soddisfino i seguenti requisiti? <ul style="list-style-type: none"> • Lunghezza minima della password di 7 caratteri • Presenza di caratteri numerici e alfabetici In alternativa, le password/passphrase devono presentare una complessità e solidità pari almeno ai parametri indicati sopra.	<ul style="list-style-type: none"> ▪ Esaminare le impostazioni di configurazione del sistema per verificare i parametri delle password 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Sì	Sì con CCW	No	N/A
8.5 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. Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema. 	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Esaminare gli elenchi di ID utente Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Sì	Sì con CCW	No	N/A
9.5 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>	<ul style="list-style-type: none"> Analizzare le politiche e le procedure per proteggere fisicamente i supporti Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6 (a) La distribuzione interna ed esterna di qualsiasi tipo di supporto è rigorosamente controllata?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure per la distribuzione dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) I controlli devono includere quanto segue:					
9.6.1 Il supporto è classificato in modo da poter determinare la sensibilità dei dati?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure per la classificazione dei supporti Consultare il personale di sicurezza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
9.6.2	Il supporto viene inviato tramite un corriere affidabile o un altro metodo di consegna che può essere adeguatamente monitorato?	<ul style="list-style-type: none"> Consultare il personale Esaminare i registri di controllo e la documentazione della distribuzione dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	L'approvazione del management viene concessa prima dello spostamento dei supporti (soprattutto quando i supporti vengono distribuiti agli individui)?	<ul style="list-style-type: none"> Consultare il personale Esaminare i registri di controllo e la documentazione della distribuzione dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	Sono in atto controlli adeguati per la memorizzazione e l'accesso ai supporti?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure di distruzione periodica dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) La distruzione dei supporti avviene in base alle seguenti modalità:					
9.8.1	(a) I materiali cartacei sono stati distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo che non sia possibile ricostruire i dati dei titolari di carta?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure di distruzione periodica dei supporti Consultare il personale Osservare i processi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I contenitori usati per conservare i materiali che contengono le informazioni da distruggere sono protetti per impedire l'accesso al contenuto?	<ul style="list-style-type: none"> Esaminare la sicurezza dei contenitori di conservazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Gestire una politica di sicurezza delle informazioni

Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale

Nota: 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.

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
12.8	Vengono mantenute e implementate politiche e procedure per gestire i provider di servizi con cui vengono condivisi i dati dei titolari di carta o che potrebbero incidere sulla sicurezza dei dati dei titolari di carta, come segue:					
12.8.1	È stato conservato un elenco di provider di servizi, inclusa una descrizione dei servizi forniti?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Osservare i processi Analizzare un elenco dei provider di servizi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	Si conserva un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati dei titolari di carta di cui entra in possesso o che memorizza, elabora o trasmette in altro modo per conto del cliente o nella misura in cui questi potrebbe avere un impatto sulla sicurezza dell’ambiente dei dati dei titolari di carta del cliente? <i>Nota: la formulazione corretta di un riconoscimento dipende dall’accordo tra le due parti, dai dettagli del servizio fornito e dalle responsabilità assegnate a ciascuna delle parti. Il riconoscimento non deve includere la formulazione corretta fornita nel presente requisito.</i>	<ul style="list-style-type: none"> Osservare i contratti scritti Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<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 “due diligence” appropriate prima dell’incarico?	<ul style="list-style-type: none"> Osservare i processi Analizzare le politiche e le procedure e la documentazione di supporto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
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?	<ul style="list-style-type: none"> ▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	Vengono conservate le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità?	<ul style="list-style-type: none"> ▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.1	(a) È stato creato un piano di risposta agli incidenti da implementare in caso di violazione del sistema?	<ul style="list-style-type: none"> ▪ Analizzare il piano di risposta agli incidenti ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Appendice A - Requisiti PCI DSS aggiuntivi

Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso

Questa appendice non viene utilizzata per le valutazioni dell'esercente.

Appendice A2 - Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale

Questa appendice non viene utilizzata per le valutazioni dell'esercente SAQ A.

Appendice A3 - Convalida aggiuntiva delle entità designate (DESV)

Questa appendice si applica solo alle entità designate da un acquirente o un marchio di pagamento che richiedono la convalida aggiuntiva di requisiti PCI DSS esistenti. Le entità che richiedono la convalida in questo appendice devono utilizzare il modello di reporting aggiuntivo DESV e l'Attestato di conformità aggiuntivo per il reporting e consultare l'acquirente e/o il marchio di pagamento applicabile per le procedure di invio.

Appendice B - 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 con CCW”.

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 allo standard PCI DSS.

Per informazioni sui controlli compensativi e per istruzioni su come completare il presente foglio di lavoro, consultare le appendici B, C e D degli 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.	

Sezione 3 -Dettagli su convalida e attestato

Parte 3. Convalida PCI DSS

Questo AOC si basa sui risultati annotati nel questionario SAQ A (Sezione 2), datato (*data di completamento SAQ*).

In base ai risultati documentati nel SAQ A indicato sopra, i firmatari di cui alle Parti 3b-3d, come applicabile, dichiarano il seguente stato di conformità dell'entità identificata nella Parte 2 di questo documento: (*selezionare un'opzione*):

<input type="checkbox"/>	<p>Conforme: Tutte le sezioni del questionario PCI DSS SAQ sono state completate e a tutte le domande è stato risposto in modo affermativo, determinando una valutazione di CONFORMITÀ globale; pertanto (<i>Ragione sociale esercente</i>) ha dimostrato la massima conformità agli standard PCI DSS.</p>						
<input type="checkbox"/>	<p>Non conforme: non tutte le sezioni del questionario PCI DSS SAQ sono state completate o non a tutte le domande è stata fornita una risposta affermativa, determinando una valutazione di NON CONFORME globale; pertanto (<i>Ragione sociale esercente</i>) non ha dimostrato la massima conformità agli standard PCI DSS.</p> <p>Data di destinazione per conformità:</p> <p>è possibile che a un'entità che invia questo modulo con lo stato "Non conforme" venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. <i>Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4.</i></p>						
<input type="checkbox"/>	<p>Conforme ma con eccezione legale: uno o più requisiti sono stati contrassegnati con "No" a causa di una restrizione legale che impedisce di rispondere al requisito. Questa opzione richiede un'ulteriore revisione da parte dell'acquirente o del marchio di pagamento.</p> <p><i>Se selezionata, completare quanto segue:</i></p> <table border="1"> <thead> <tr> <th>Requisito interessato</th> <th>Dettagli su come il vincolo legale impedisce la conformità ai requisiti</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti				
Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti						

Parte 3a. Riconoscimento dello stato

I firmatari confermano:

(*Selezionare tutte le risposte pertinenti*)

<input type="checkbox"/>	Il questionario di autovalutazione PCI DSS A, versione (<i>versione 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 in ogni momento, in base a quanto applicabile al mio ambiente.
<input type="checkbox"/>	Se il mio ambiente cambia, accetto di dover rivalutare l'ambiente e implementare eventuali requisiti PCI DSS in base alle necessità.

Parte 3a. Riconoscimento dello stato (continua)

- | | |
|--------------------------|---|
| <input type="checkbox"/> | Nessuna prova della memorizzazione dei dati della traccia completa ¹ , dei dati CAV2, CVC2, CID o CVV2 ² oppure dei dati PIN ³ dopo che l'autorizzazione alla transazione è stata individuata su QUALSIASI sistema esaminato durante questa valutazione. |
| <input type="checkbox"/> | Le scansioni ASV vengono completate dal Fornitore di prodotti di scansione approvato (ASV) PCI SSC (Nome ASV) |

Parte 3b. Attestato esercente

Firma del funzionario esecutivo dell'esercente ↑

Data:

Nome del funzionario esecutivo dell'esercente:

Mansione:

Parte 3c. Riconoscimento dell'azienda qualificata per la valutazione (QSA) (se applicabile)

Se un QSA è stato coinvolto o aiutato durante questa valutazione, descrivere il ruolo ricoperto:

Firma del funzionario espressamente autorizzato dell'azienda QSA ↑

Data:

Nome del funzionario espressamente autorizzato:

Azienda QSA:

Parte 3d. Coinvolgimento dell'azienda interna per la valutazione (ISA) (se applicabile)

Se un ISA è stato coinvolto o aiutato durante questa valutazione, identificare il personale ISA e descrivere il ruolo ricoperto:

¹ 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 i dati della traccia completa dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il PAN, la data di scadenza e il nome del titolare della carta.

² Il valore di tre o quattro cifre stampato nel riquadro della firma o nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

³ Numero di identificazione personale inserito dal titolare della carta durante una transazione con carta presente e/o blocco PIN cifrato presente all'interno del messaggio di transazione.

Parte 4. Piano d'azione per i requisiti non conformi

Selezionare la risposta appropriata per “Conforme ai requisiti PCI DSS” per ogni requisito. In caso di risposta negativa a uno dei requisiti, è necessario fornire la data in cui si prevede che 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.

Requisito* PCI DSS	Descrizione del requisito	Conforme ai requisiti PCI DSS (Selezionarne uno)		Data della soluzione e azioni (Se è stata selezionata l'opzione “NO” per un qualsiasi requisito)
		SÌ	NO	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
8	Individuare e autenticare l'accesso ai componenti di sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	<input type="checkbox"/>	<input type="checkbox"/>	

** I requisiti PCI DSS indicati qui fanno riferimento alle domande della Sezione 2 del questionario SAQ.*

