Settore delle carte di pagamento (PCI)
Standard di protezione dei dati

Questionario di autovalutazione P2PE e Attestato di conformità

Esercenti che utilizzano terminali di pagamento hardware in una soluzione P2PE inclusa nell'elenco PCI SSC - Nessuna memorizzazione elettronica dei dati dei titolari di carta

Per l'uso con PCI DSS versione 3.2.1

Giugno 2018

Modifiche del documento

Data	Versione PCI DSS	Revisione SAQ	Descrizione
N/A	1.0		Non utilizzata.
Maggio 2012	2.0		Creare un SAQ P2PE-HW per esercenti che utilizzano esclusivamente terminali hardware nell'ambito di una soluzione P2PE convalidata inclusa nell'elenco da PCI SSC. Questo questionario SAQ va utilizzato con 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 allinearlo a PCI DSS v3.1. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a *PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.0 alla 3.1*. Rimosso "HW" dal titolo SAQ, poiché può essere utilizzato da esercenti che sfruttano sia la soluzione P2PE HW/HW che HW/Hybrid.
Luglio 2015	3.1	1.1	Aggiornato per rimuovere i riferimenti alle "migliori pratiche" prima del 30 giugno 2015.
Aprile 2016	3.2	1.0	Aggiornato per allinearlo a PCI DSS v3.2. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a *PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.1 alla 3.2*. Rimozione dei Requisiti PCI DSS 3.3 e 4.2, come trattato nell'implementazione della soluzione PCI P2PE e PIM.
Gennaio 2017	3.2	1.1	Modifiche al documento aggiornato al fine di chiarire i requisiti rimossi nell'aggiornamento di Aprile 2016.
Giugno 2018	3.2.1	1.0	Aggiornato per allinearlo a PCI DSS v3.2.1. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a *PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.2 alla 3.2.1.*

ATTESTAZIONE:

La versione testuale in lingua inglese di questo documento, nella forma in cui quest'ultima è stata pubblicata sul sito Internet PCI SSC, verrà, a tutti gli effetti, considerata la versione ufficiale di questi documenti. Qualora dovessero insorgere ambiguità o incongruenze fra questo testo e il testo in lingua inglese, prevarrà in tal sede la versione anglofona.

Sommario

Operazioni preliminari

Criteri di idoneità degli esercenti per il questionario SAQ P2PE

SAQ P2PE è stato sviluppato per rispondere ai requisiti applicabili agli esercenti che elaborano i dati dei titolari di carta esclusivamente tramite terminali di pagamento hardware inclusi in una soluzione P2PE (Point-to-Point Encryption) convalidata e inclusa nell'elenco PCI.

Gli esercenti SAQ P2PE non dispongono dell'accesso ai dati dei titolari di carta con testo in chiaro su alcun sistema informatico e inseriscono i dati degli account tramite terminali di pagamento hardware presenti in una soluzione P2PE approvata PCI SSC. Gli esercenti SAQ P2PE possono essere punti vendita reali (con presenza fisica della carta) o società di vendita per posta/telefono (senza presenza fisica della carta). Ad esempio, una società di vendita per posta/telefono potrebbe essere idonea al SAQ P2PE se riceve i dati dei titolari di carta in formato cartaceo o per telefono e se attribuisce loro una chiave direttamente ed esclusivamente in un dispositivo hardware convalidato P2PE.

Gli esercenti SAQ P2PE confermano che, per questo canale di pagamento:

- Tutte le operazioni di elaborazione di pagamento avvengono tramite una soluzione P2PE convalidata che è stata approvata e inclusa nell'elenco da PCI SSC.
- Gli unici sistemi presenti nell'ambiente dell'esercente che memorizzano, elaborano o trasmettono i dati degli account sono i dispositivi di punto di interazione (POI), approvati per essere utilizzati con la soluzione P2PE convalidata e inclusa nell'elenco PCI.
- L'azienda non riceve o trasmette in altro modo i dati dei titolari di carta in formato elettronico;
- L'azienda verifica che non sia presente alcuna memorizzazione precedente dei dati dei titolari di carta all'interno dell'ambiente.
- 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.
- La società ha implementato tutti i controlli presenti in *P2PE Instruction Manual (PIM)* fornito dal provider della soluzione P2PE.

Questo SAQ non è applicabile ai canali di e-commerce.

Questa versione più breve del questionario di autovalutazione comprende domande che riguardano un tipo specifico di ambiente di esercenti di dimensioni ridotte, secondo quando 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.

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. Confermare di avere implementato tutti gli elementi presenti nel PIM.
4. Valutare il proprio ambiente per la conformità ai requisiti PCI DSS applicabili.
5. 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 P2PE)
- Sezione 3 (Parti 3 e 4 dell'AOC) - Dettagli su convalida e attestato e piano d'azione per i requisiti non conformi (se applicabile)

6. Inviare il questionario SAQ e l'attestato di conformità (AOC), insieme ad eventuale altra documentazione richiesta, 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 *(Requisiti PCI DSS e procedure di valutazione della sicurezza)*	▪ 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	▪ Informazioni su tutti i questionari SAQ e sui relativi criteri di idoneità ▪ Come determinare quale questionario SAQ è adatto alla propria azienda
Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS	▪ 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)	Il test previsto è stato eseguito e il requisito risulta soddisfatto grazie all'ausilio di un controllo compensativo. Tutte le risposte di questa colonna richiedono il completamento di un Foglio di lavoro - Controllo compensativo (CCW) presente nell'Appendice B del questionario SAQ. 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.
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)	Il requisito non si applica all'ambiente dell'azienda. (Per consultare alcuni esempi, vedere la *Guida per la non applicabilità di determinati requisiti specifici* riportata di seguito.) Tutte le risposte di questa colonna richiedono una spiegazione di supporto disponibile nell'Appendice C del questionario SAQ.

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 ☐ Ordini via posta/telefono (MOTO) ☐ Altro (specificare):

Quali tipi di canali di pagamento offre l'azienda?	Quali sono i canali di pagamento coperti dal presente questionario SAQ?
☐ Ordini via posta/telefono (MOTO)	☐ Ordini via posta/telefono (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Con carta presente (contatto diretto)	☐ 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 2. Riepilogo esecutivo *(continua)*

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

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

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

Parte 2d. Soluzione P2PE

Fornire le seguenti informazioni relative alla soluzione P2PE PCI convalidata utilizzata dalla propria azienda:

Nome del provider della soluzione P2PE:	
Nome della soluzione P2PE:	
Numero di riferimento PCI SSC	
Dispositivi POI P2PE elencati utilizzati dall'esercente (dipendenze dei dispositivi PTS):	

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? *(Consultare la sezione "Segmentazione di rete" di PCI DSS per indicazioni sulla segmentazione di rete.)*	☐ Sì ☐ No

Parte 2. Riepilogo esecutivo *(continua)*

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, 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 questionario SAQ P2PE

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

☐	Tutte le operazioni di elaborazione di pagamento avvengono tramite la soluzione P2PE PCI convalidata che è stata approvata e e inclusa nell'elenco da PCI SSC (secondo quanto detto sopra).
☐	Gli unici sistemi presenti nell'ambiente dell'esercente che memorizzano, elaborano o trasmettono i dati degli account sono i dispositivi di punto di interazione (POI), approvati per essere utilizzati con la soluzione P2PE convalidata e inclusa nell'elenco PCI.
☐	L'esercente non riceve o trasmette in altro modo i dati dei titolari di carta in formato elettronico.
☐	L'esercente verifica che non sia presente alcuna memorizzazione precedente dei dati dei titolari di carta all'interno dell'ambiente.
☐	L'esercente conserva i dati dei titolari di carta solo in forma di resoconti o copie di ricevute cartacee e non in formato elettronico.
☐	L'esercente ha implementato tutti i controlli presenti in P2PE Instruction Manual (PIM) fornito dal provider della soluzione P2PE.

Sezione 2 - Questionario di autovalutazione P2PE

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*. Dal momento che viene fornito solo un sottoinsieme di requisiti PCI DSS in questo questionario SAQ P2PE, è possibile che le domande non siano numerate in maniera consecutiva.*

Data di completamento dell'autovalutazione:

Protezione dei dati dei titolari di carta

Requisito 3 - Proteggere i dati dei titolari di carta memorizzati

Nota*: Il Requisito 3 si applica solo agli esercenti SAQ P2PE che dispongono di record cartacei (ad esempio, ricevute, report cartacei ecc.) contenenti dati di account, inclusi i numeri di conto primari (primary account numbers, PAN).*

	Domanda PCI DSS	Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
3.1	Le politiche, le procedure e i processi per la conservazione e l'eliminazione dei dati sono implementati come indicato di seguito:					
	(a) La quantità dei dati memorizzati e il tempo di conservazione sono limitati in base alle esigenze aziendali, legali e/o legislative?	▪ Analizzare le politiche e le procedure per la conservazione e l'eliminazione dei dati ▪ Consultare il personale.	☐	☐	☐	☐
	(b) Sono stati adottati processi definiti per l'eliminazione sicura dei dati dei titolari di carta quando questi dati non sono più necessari per scopi legali, legislativi e/o aziendali?	▪ Analizzare le politiche e le procedure ▪ Consultare il personale. ▪ Esaminare il meccanismo di eliminazione	☐	☐	☐	☐
	(c) Sono presenti requisiti specifici di conservazione dei dati dei titolari di carta? *Ad esempio, è necessario conservare i dati dei titolari di carta per un periodo X per scopi aziendali Y.*	▪ Analizzare le politiche e le procedure ▪ Consultare il personale. ▪ Esaminare i requisiti di conservazione	☐	☐	☐	☐
	(d) È presente un processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti?	▪ Analizzare le politiche e le procedure ▪ Consultare il personale. ▪ Osservare i processi di eliminazione	☐	☐	☐	☐

	Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
	(e) Tutti i dati dei titolari di carta memorizzati soddisfano i requisiti contenuti nella politica di conservazione dei dati?	▪ Esaminare i file e i record del sistema	☐	☐	☐	☐
Istruzioni: *le risposte "Sì" alle domande per i requisiti al punto 3.1 indicano che se un esercente memorizza documenti cartacei (ad esempio, ricevute o report cartacei) contenenti i dati di account, l'**esercente** memorizza i documenti cartacei solo per il tempo necessario per scopi aziendali, legali e/o legislativi e li distrugge quando non vengono più utilizzati.* *Se l'**esercente** non stampa né conserva i documenti cartacei contenenti i dati di account, deve contrassegnare la colonna "N/A" e completare il foglio di lavoro "Spiegazione di non applicabilità" presente nell'Appendice C.*						
3.2.2	Per la conservazione di tutti i documenti cartacei, 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 dopo l'autorizzazione?	▪ Esaminare le origini dei dati dei documenti cartacei	☐	☐	☐	☐
Istruzioni: Istruzioni: *una risposta "Sì" al Requisito 3.2.2 indica che se un esercente annota il codice di sicurezza della carta durante l'**esecuzione** di una transazione, l'**esercente** distrugge in sicurezza i documenti cartacei (ad esempio, con un tritadocumenti) al termine della transazione oppure oscura il codice (ad esempio, coprendolo con un pennarello) prima di memorizzarli.* *Se l'**esercente** non richiede mai il numero di tre o quattro cifre impresso sulla parte anteriore o sul retro di una carta di pagamento ("**codice** di sicurezza della **carta**"), deve contrassegnare la colonna "N/A" e completare il foglio di lavoro "**Spiegazione** di non **applicabilità**" presente nell'**Appendice** C.*						
3.7	Le politiche di sicurezza e le procedure operative per la protezione dei dati dei titolari di carta sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Analizzare le politiche di sicurezza e le procedure operative ▪ Consultare il personale.	☐	☐	☐	☐
Istruzioni: Istruzioni: *una risposta "Sì" al Requisito 3.7 significa che se l'**esercente** memorizza i documenti cartacei dei dati di account, ha adottato politiche e procedure in relazione ai Requisiti 3.1, 3.2.2 e 3.3. Questo serve a garantire che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative documentate per la gestione continua della memorizzazione sicura dei dati dei titolari di carta.*						

Implementazione di rigide misure di controllo dell'accesso

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

Nota: *I Requisiti 9.5 e 9.8 si applicano solo agli esercenti SAQ P2PE che dispongono di record cartacei (ad esempio, ricevute, report cartacei ecc.) contenenti dati di account, inclusi i numeri di conto primari (primary account numbers, PAN).*

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)? *Ai fini del Requisito 9, per "supporti" si intendono tutti i supporti elettronici e cartacei contenenti dati di titolari di carta.*	▪ Analizzare le politiche e le procedure per proteggere fisicamente i supporti ▪ Consultare il personale.	☐	☐	☐	☐
9.8	(f) Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?	▪ Analizzare le politiche e le procedure di distruzione periodica dei supporti	☐	☐	☐	☐
	(c) La distruzione dei supporti avviene in base alle seguenti modalità:					
9.8.1	(g) 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?	▪ Analizzare le politiche e le procedure di distruzione periodica dei supporti ▪ Consultare il personale. ▪ Osservare i processi	☐	☐	☐	☐
	(b) I contenitori usati per conservare i materiali che contengono le informazioni da distruggere sono protetti per impedire l'accesso al contenuto?	▪ Analizzare le politiche e le procedure di distruzione periodica dei supporti ▪ Esaminare la sicurezza dei contenitori di conservazione	☐	☐	☐	☐

Domanda PCI DSS	Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
		Sì	**Sì con CCW**	**No**	**N/A**
Istruzioni: *le risposte "Sì" per i requisiti 9.5 e 9.8 significano che l'esercente conserva in modo sicuro tutti i documenti cartacei contenenti i dati di account; ad esempio li ripone in un cassetto, armadietto o in una cassaforte chiusi a chiave e li distrugge quando non sono più necessari per scopi aziendali. Ciò include un documento o una politica scritti per i dipendenti che spieghi loro come tutelare i documenti cartacei che contengono i dati di account e come distruggerli quando non vengono più utilizzati.* *Se l'esercente non conserva i documenti cartacei contenenti i dati di account, deve contrassegnare la colonna "N/A" e completare il foglio di lavoro "Spiegazione di non applicabilità" presente nell'Appendice C.*					
9.9 I dispositivi che acquisiscono i dati delle carte di pagamento attraverso un'interazione fisica diretta con la carta vengono protetti contro manomissioni e sostituzioni, come indicato di seguito? ***Nota:*** *questo requisito si applica ai dispositivi che leggono le carte utilizzati nelle transazioni con carta presente (ovvero, tessera magnetica o dip) nel punto vendita. Questo requisito non si applica ai componenti per l'immissione manuale, quali tastiere di computer o tastierini di POS.*					
(a) Le politiche e le procedure prevedono che venga conservato un elenco di tali dispositivi?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
(b) Le politiche e le procedure richiedono che i dispositivi siano sottoposti a un'ispezione periodica per controllare eventuali manomissioni o sostituzioni?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
(c) Le politiche e le procedure impongono la corretta formazione del personale che deve essere a conoscenza del comportamento sospetto e segnalare le manomissioni o le sostituzioni dei dispositivi?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
9.9.1 (a) L'elenco dei dispositivi include quanto segue? – Marca, modello del dispositivo – Posizione del dispositivo (ad esempio, l'indirizzo della sede o della struttura in cui si trova il dispositivo) – Numero di serie del dispositivo o altro metodo di identificazione univoca	▪ Esaminare l'elenco dei dispositivi	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(b) L'elenco è accurato e aggiornato?	▪ Osservare i dispositivi e le relative posizioni e confrontarli con l'elenco	☐	☐	☐	☐
	(c) L'elenco di dispositivi viene aggiornato quando i dispositivi vengono aggiunti, riposizionati, messi fuori uso ecc.?	▪ Consultare il personale.	☐	☐	☐	☐
9.9.2	(a) Le superfici del dispositivo vengono ispezionate periodicamente per rilevare manomissioni (ad esempio, aggiunta di skimmer di carte ai dispositivi) o sostituzioni (ad esempio, controllando il numero di serie o le caratteristiche del dispositivo per verificare che non sia stato sostituito con un dispositivo fraudolento), come indicato di seguito? ***Nota:*** *esempi di indicazioni che un dispositivo potrebbe essere stato alterato o sostituito includono raccordi o cavi innestati nel dispositivo, etichette di sicurezza mancanti o modificate, involucri rotti o di colori diversi o modifiche al numero di serie o altri contrassegni esterni.*	▪ Consultare il personale. ▪ Osservare i processi di ispezione e confrontare con processi definiti	☐	☐	☐	☐
	(b) Il personale è a conoscenza delle procedure per ispezionare i dispositivi?	▪ Consultare il personale.	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	**Sì con CCW**	**No**	**N/A**
9.9.3	Il personale è stato debitamente formato per essere a conoscenza dei tentativi di alterazione o sostituzione dei dispositivi, con inclusione di quanto segue?					
	(a) Il materiale formativo per il personale dei punti vendita include quanto segue? – Verifica dell'identità di eventuali terzi che sostengono di essere addetti alle riparazioni o alla manutenzione, prima di consentire loro l'autorizzazione a modificare o risolvere i problemi dei dispositivi. – Divieto di installare, sostituire o restituire dispositivi in assenza di verifica. – Massima attenzione al comportamento sospetto in prossimità dei dispositivi (ad esempio, tentativi di persone sconosciute di disconnettere o aprire i dispositivi). – Segnalazione di comportamento sospetto e indicazioni di alterazione o sostituzione del dispositivo al personale appropriato (ad esempio, un manager o un addetto alla sicurezza).	▪ Analizzare i materiali di formazione	☐	☐	☐	☐
9.9.3 *(cont.)*	(b) Il personale dei punti vendita ha seguito la giusta formazione e conosce le procedure necessarie per individuare e segnalare i tentativi di manomissione o sostituzione dei dispositivi?	▪ Consultare il personale presso le sedi POS	☐	☐	☐	☐
Istruzioni: *le risposte "Sì" ai requisiti di cui al punto 9.9 indicano che l'**esercente** ha adottato politiche e procedure in relazione ai Requisiti 9.9.1-9.9.3 e che l'**esercente** gestisce un elenco aggiornato di dispositivi, conduce ispezioni periodiche dei dispositivi e forma i dipendenti in merito a cosa controllare per rilevare dispositivi manomessi o sostituiti.*						
9.10	Le politiche di sicurezza e le procedure operative per la limitazione dell'accesso fisico ai dati dei titolari di carta sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Esaminare le politiche di sicurezza e le procedure operative ▪ Consultare il personale.	☐	☐	☐	☐

Domanda PCI DSS	Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
		Sì	Sì con CCW	No	N/A
Istruzioni: *una risposta "Sì" al Requisito 9.10 significa che l'**esercente** ha adottato politiche e procedure in relazione ai Requisiti 9.5, 9.8 e 9.9, come applicabile in base al proprio ambiente. Questo serve a garantire che il personale conosca e applichi le politiche di sicurezza e le procedure operative documentate.*					

Gestione di una politica di sicurezza delle informazioni

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

Nota: *il Requisito 12 specifica che gli esercenti devono adottare politiche di sicurezza delle informazioni per il proprio personale; tali politiche possono tuttavia essere tanto semplici o complesse quanto richiesto dalle dimensioni e dalla complessità delle attività dell'esercente. Il documento contenente le politiche deve essere fornito a tutto il personale affinché sia a conoscenza delle proprie responsabilità in merito alla protezione dei terminali di pagamento, dei documenti cartacei con i dati dei titolari di carta ecc. Se un esercente non ha personale alle sue dipendenze, dovrà comprendere e accettare la propria responsabilità per la sicurezza all'interno del punto vendita.*

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
12.1	È stata definita, pubblicata, gestita e diffusa una politica per la sicurezza tra tutto il personale interessato?	▪ Analizzare la politica di sicurezza delle informazioni	☐	☐	☐	☐
12.1.1	La politica di sicurezza viene rivista almeno una volta all'anno e aggiornata quando l'ambiente cambia?	▪ Analizzare la politica di sicurezza delle informazioni ▪ Consultare il personale responsabile.	☐	☐	☐	☐
Istruzioni: *le risposte "Sì" ai requisiti del punto 12.1 indicano che l'esercente ha adottato una politica di sicurezza ritenuta ragionevole per le dimensioni e la complessità delle attività che svolge e che tale politica viene rivista ogni anno e aggiornata qualora necessario. Ad esempio, la politica può essere un semplice documento che spiega come proteggere il punto vendita e i dispositivi di pagamento in conformità a* P2PE Instruction Manual (PIM) *e chi contattare in caso di emergenza.*						
12.4	La politica e le procedure per la sicurezza delle informazioni definiscono chiaramente le responsabilità in termini di protezione delle informazioni per tutto il personale?	▪ Analizzare le politiche e le procedure di sicurezza delle informazioni ▪ Consultare un campione di personale responsabile	☐	☐	☐	☐
Istruzioni: *una risposta "Sì" al Requisito 12.4 significa che la politica di sicurezza dell'esercente definisce le responsabilità di base di tutto il personale, in conformità alle dimensioni e alla complessità delle attività che svolge. Ad esempio, le responsabilità relative alla sicurezza possono essere definite in base alle responsabilità di base specificate per livello dei dipendenti, come le responsabilità previste per un manager/titolare e quelle previste per gli impiegati.*						
12.5	Le seguenti responsabilità per la gestione della sicurezza delle informazioni sono state assegnate a una singola persona o a un team?					

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	**Sì con CCW**	**No**	**N/A**
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?	▪ Analizzare le politiche e le procedure di sicurezza delle informazioni	☐	☐	☐	☐
Istruzioni: *una risposta "Sì" al Requisito 12.5.3 indica che l'**esercente** ha nominato una persona come responsabile del piano di risposta agli incidenti e di escalation come previsto al punto 12.9.*						
12.6	(a) È in atto un programma formale di consapevolezza della sicurezza per rendere tutto il personale consapevole delle procedure e dei criteri di protezione dei dati dei titolari di carta?	▪ Analizzare il programma di consapevolezza della sicurezza	☐	☐	☐	☐
Istruzioni: *una risposta "Sì" al Requisito 12.6 indica che l'**esercente** ha adottato un programma per la consapevolezza sulla sicurezza, conforme alle dimensioni e alla complessità delle attività che svolge. A esempio, un programma semplice per la sicurezza potrebbe essere un volantino esposto nel backoffice o un messaggio e-mail periodico inviato a tutti i dipendenti. Esempi di messaggi per i programmi sulla consapevolezza comprendono descrizioni dei suggerimenti sulla sicurezza che tutti i dipendenti devono seguire, ad es. come bloccare le porte e i contenitori, come determinare se un terminale è stato manomesso e come identificare il personale autorizzato a eseguire interventi di manutenzione sull'**hardware** dei terminali.*						
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?	▪ Analizzare le politiche e le procedure ▪ Osservare i processi ▪ Analizzare un elenco dei provider di servizi	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	**Sì con CCW**	**No**	**N/A**
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? ***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.*	▪ Osservare i contratti scritti ▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
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?	▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto	☐	☐	☐	☐
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?	▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto	☐	☐	☐	☐
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?	▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto	☐	☐	☐	☐

Istruzioni: *le risposte "Sì" alle domande per i requisiti al punto 12.8 indicano che l'**esercente** dispone di un elenco di provider di servizi con cui ha stretto accordi e condivide i dati dei titolari di carta. Ad esempio, tali accordi potrebbero essere applicabili se un esercente si rivolge a una società di conservazione documenti per archiviare i documenti cartacei contenenti i dai di account.*

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	**Sì con CCW**	**No**	**N/A**
12.10.1	(a) È stato creato un piano di risposta da implementare in caso di violazione del sistema?	▪ Analizzare il piano di risposta agli incidenti ▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
Istruzioni: *le risposte "Sì" ai requisiti del punto 12.10 indicano che l'**esercente** ha documentato una piano di risposta agli incidenti ed escalation da adottare per le emergenze conforme alle dimensioni e alla complessità delle attività che svolge. Ad esempio, tale piano può essere un documento semplice esposto nel backoffice con un elenco delle persone da contattare in una serie di situazioni e che viene rivisto a cadenza annuale per confermare che sia ancora accurato. Potrebbe però anche estendersi a un piano di risposta agli incidenti completo che comprende strutture "**hotsite**" di backup e test annuale completo. Questo piano deve essere facilmente reperibile da tutto il personale come risorsa in caso di emergenza.*						

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 per connessioni a terminale POI POS con carta presente

Questa appendice non viene utilizzata per le valutazioni dell'esercente SAQ P2PE.

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.	

Appendice C - Spiegazione di non applicabilità

Se è stata selezionata la colonna "N/A" (Non applicabile) del questionario, utilizzare questo foglio di lavoro per spiegare il motivo per cui il requisito descritto non è applicabile alla propria azienda.

Requisito	Motivo per cui il requisito non è applicabile
Esempio:	
12.8	I dati di titolari di carta non sono mai condivisi con provider di servizi.

Sezione 3 - Dettagli su convalida e attestato

Parte 3. Convalida PCI DSS

Questo AOC si basa sui risultati annotati nel questionario SAQ P2PE (Sezione 2), datato *(data di completamento SAQ).*

In base ai risultati documentati nel questionario SAQ P2PE 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):***

☐	**Conforme:** Tutte le sezioni del questionario PCI DSS SAQ P2PE sono state completate e a tutte le domande è stato risposto in modo affermativo, determinando una valutazione di **CONFORMITÀ** globale; pertanto *(Ragione sociale esercente)* ha dimostrato la massima conformità agli standard PCI DSS.
☐	**Non conforme:** non tutte le sezioni del questionario PCI DSS SAQ P2PE sono state completate o non a tutte le domande è stata fornita una risposta affermativa, determinando una valutazione di **NON CONFORME** globale; **pertanto** (Ragione sociale esercente) *non ha dimostrato la massima conformità agli standard PCI DSS*. **Data di destinazione** 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.*
☐	**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. *Se selezionata, completare quanto segue:* **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)

☐	Il questionario di autovalutazione PCI DSS P2PE, versione *(versione di SAQ)*, 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 sotto tutti gli aspetti.
☐	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.
☐	Se il mio ambiente cambia, accetto di dover rivalutare l'ambiente e implementare eventuali requisiti PCI DSS in base alle necessità.

Parte 3. Convalida PCI DSS *(continua)*

Parte 3a. Riconoscimento dello stato *(continua)*

☐	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.

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, perché non tutti i marchi di pagamento richiedono questa sezione.

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**	
3	Proteggere i dati di titolari di carta memorizzati.	☐	☐	
9	Limitare l'accesso fisico ai dati di titolari di carta.	☐	☐	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale.	☐	☐	

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