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

Questionario di autovalutazione C-VT e Attestato di conformità

Esercenti con terminali di pagamento virtuali basati su Web - Nessuna memorizzazione elettronica dei dati di titolari di carta

Per l'uso con PCI DSS versione 3.2

Aprile 2016

Modifiche del documento

Data	Versione PCI DSS	Revisione 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 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*.
Luglio 2015	3.1	1.1	Numerazione delle versioni aggiornata per allinearla ad altri questionari SAQ.
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.*

Sommario

Modifiche del documento ..... **ii**

Operazioni preliminari ..... **iii**

Passaggi per il completamento dell'autovalutazione PCI DSS ..... **iv**

Comprensione del questionario di autovalutazione ..... **iv**

Test previsti ..... *iv*

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 C-VT **4**

Sviluppo e gestione di sistemi e reti sicure **4**

Requisito 1 - Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta *4*

Requisito 2 - Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione *6*

Protezione dei dati dei titolari di carta **10**

Requisito 3 - Proteggere i dati dei titolari di carta memorizzati *10*

Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche *12*

Utilizzare un programma per la gestione delle vulnerabilità **14**

Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus *14*

Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette *16*

Implementazione di rigide misure di controllo dell'accesso **17**

Requisito 7 - Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario *17*

Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema *18*

Requisito 9 - Limitare l'accesso fisico ai dati dei titolari di carta *20*

Gestire una politica di sicurezza delle informazioni **22**

Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale *22*

Appendice A - Requisiti PCI DSS aggiuntivi **25**

Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso *25*

Appendice A2 - Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale *25*

Appendice A3 - Convalida aggiuntiva delle entità designate (DESV) *26*

Appendice B - Foglio di lavoro - Controlli compensativi **27**

Appendice C - Spiegazione di non applicabilità **28**

Sezione 3 - Dettagli su convalida e attestato **29**

Operazioni preliminari

Il questionario SAQ C-VT è stato sviluppato per rispondere ai requisiti applicabili a tutti gli esercenti che elaborano i dati dei titolari di carta solo mediante terminali virtuali isolati su computer connessi a Internet.

Un terminale virtuale è un accesso basato su browser Web al sito Web di un acquirente, elaboratore o provider di servizi di terzi per autorizzare le transazioni della carta di pagamento, in cui l'esercente inserisce manualmente i dati della carta mediante un browser Web connesso in modo sicuro. A differenza dei terminali fisici, i terminali di pagamento virtuali non leggono i dati direttamente da una carta di pagamento. Dal momento che le transazioni della carta di pagamento sono inserite manualmente, i terminali di pagamento virtuali sono in genere usati al posto dei terminali fisici in ambienti di esercenti con un volumi limitati di transazioni.

Gli esercenti SAQ C-VT elaborano i dati dei titolari di carta solo tramite un terminale virtuale e non memorizzano tali dati su alcun computer. Questi terminali virtuali sono connessi a Internet per accedere a terze parti che ospitano la funzione di elaborazione del pagamento del terminale virtuale. Questa terza parte può essere un elaboratore, un acquirente o un altro provider di servizi di terzi che memorizza, elabora e/o trasmette i dati dei titolari di carta per autorizzare e/o contabilizzare le transazioni di pagamento del terminale virtuale dell'esercente.

L'applicazione di questa opzione SAQ riguarda solo gli esercenti che inseriscono manualmente una singola transazione per volta con una tastiera in una soluzione di terminale virtuale basato su Web. Gli esercenti SAQ C-VT possono essere punti vendita reali (con presenza fisica della carta) o società di vendita per posta/telefono (senza presenza fisica della carta).

Gli esercenti SAQ C-VT confermano che, per questo canale di pagamento:

- L'unica elaborazione di pagamenti della società viene effettuata mediante un terminale virtuale a cui si accede mediante un browser Web collegato ad Internet.
- La soluzione di terminale virtuale della società è fornita ed ospitata da un provider di servizi di terze parti convalidato PCI DSS.
- La società accede alla soluzione di terminale virtuale conforme PCI DSS via computer ed è isolata in un'unica posizione e non è collegata ad altre posizioni o sistemi nell'ambito del suo ambiente (ciò si può ottenere mediante segmentazione di rete o firewall per isolare il computer dagli altri sistemi).
- Il computer della società non ha software installato che determina la memorizzazione dei dati dei titolari di carta (ad esempio, non vi è alcun software per elaborazione batch o store-and-forward).
- Il computer della società non dispone di alcun dispositivo hardware collegato che viene usato per acquisire o memorizzare i dati dei titolari di carta (ad esempio non è collegato alcun lettore di carte).
- La società non riceve o trasmette in altro modo i dati dei titolari di carta elettronicamente tramite alcun canale (ad esempio mediante una rete interna o Internet).
- 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 non memorizza i dati di titolari di carta in formato elettronico.

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. 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 C-VT)
   - 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 *(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

Sebbene molte aziende che completano il questionario SAQ C-VT debbano convalidare la propria conformità a ogni requisito PCI DSS incluso nel questionario, alcune aziende con modelli di business molto specifici possono trovare non applicabili alcuni requisiti. Ad esempio, una società che non utilizza una tecnologia wireless in alcun modo non può garantire la conformità ai requisiti indicati nelle sezioni degli standard PCI DSS specifiche per la gestione di tale tecnologia (ad esempio Requisiti 1.2.3, 2.1.1 e 4.1.1).

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?	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 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 e riepilogo delle sedi (ad esempio, punti vendita, uffici, centri dati, call center ecc.) 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. 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)
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ 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? *(Consultare la sezione "Segmentazione di rete" di PCI DSS per indicazioni sulla segmentazione di rete.)*	☐ Sì ☐ No

Parte 2f. Provider di servizi di terzi	
L'azienda utilizza un responsabile dell'integrazione e rivenditore qualificati (QIR)? Se sì: Nome dell'azienda QIR: Singolo nome QIR: Descrizione dei servizi forniti dal QIR:	☐ Sì ☐ No
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 C-VT	
L'esercente dichiara la propria idoneità per il completamento di questa versione più breve del questionario di autovalutazione perché, per questo canale:	
☐	L'unica elaborazione di pagamenti dell'esercente viene effettuata mediante un terminale virtuale a cui si accede mediante un browser Web collegato ad Internet.
☐	La soluzione di terminale virtuale dell'esercente è fornita ed ospitata da un provider di servizi di terze parti convalidato PCI DSS.
☐	L'esercente accede al terminale virtuale conforme a PCI DSS tramite un computer che è isolato in una posizione unica e non è collegato ad altre posizioni o sistemi all'interno del proprio ambiente.
☐	Il computer dell'esercente non dispone di software installato che determina la memorizzazione dei dati dei titolari di carta (ad esempio, non vi è alcun software per elaborazione batch o store-and-forward).
☐	Il computer dell'esercente non dispone di alcun dispositivo hardware collegato usato per acquisire o memorizzare i dati dei titolari di carta (ad esempio non è collegato alcun lettore di carte).
☐	L'esercente non riceve o trasmette in altro modo i dati dei titolari di carta elettronicamente tramite alcun canale (ad esempio mediante una rete interna o Internet).
☐	L'esercente non memorizza dati dei titolari di carta in formato elettronico.
☐	L'esercente conserva i dati dei titolari di carta solo in forma di resoconti o copie di ricevute cartacee e non in formato elettronico.

Sezione 2 - Questionario di autovalutazione C-VT

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

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
1.2	Le configurazioni di firewall e router limitano le connessioni tra le reti non attendibili e qualsiasi sistema nell'ambiente dei dati di titolari di carta nel modo seguente: ***Nota:*** *una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.*					
1.2.1	(a) Il traffico in entrata e in uscita è limitato a quello indispensabile per l'ambiente dei dati dei titolari di carta?	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
	(b) Il resto del traffico in entrata e in uscita viene negato in modo specifico, ad esempio utilizzando un comando esplicito "deny all" o un comando implicito di negazione dopo un'istruzione "allow".	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
1.2.3	Sono stati installati i firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e tali firewall sono stati configurati in modo da negare o controllare (se necessario per gli scopi aziendali) solo il traffico autorizzato tra l'ambiente wireless e l'ambiente dei dati dei titolari di carta?	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
1.3	È vietato l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta, come segue:					
1.3.4	Viene autorizzato in modo esplicito il traffico in uscita dall'ambiente dei dati di titolari di carta ad Internet?	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
1.3.5	Sono consentite nella rete solo le connessioni già stabilite?	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
1.4	(a) È stato installato ed è attivo il firewall personale (o funzionalità equivalente) su tutti i dispositivi mobili (inclusi quelli di proprietà dell'azienda e/o dei dipendenti) con connettività a Internet se all'esterno della rete (ad esempio, laptop utilizzati dai dipendenti) e quali vengono utilizzati anche per accedere al CDE?	▪ Analizzare le politiche e gli standard di configurazione ▪ Esaminare i dispositivi mobili e/o di proprietà dei dipendenti	☐	☐	☐	☐
	(b) Il firewall personale (o funzionalità equivalente) è configurato in base a impostazioni specifiche, è in esecuzione in modo attivo e non è modificabile da parte degli utenti di dispositivi mobili e/o di proprietà dei dipendenti?	▪ Analizzare le politiche e gli standard di configurazione ▪ Esaminare i dispositivi mobili e/o di proprietà dei dipendenti	☐	☐	☐	☐

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? *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.*	▪ Analizzare le politiche e le procedure ▪ Esaminare la documentazione del fornitore ▪ Osservare le configurazioni di sistema e le impostazioni account ▪ Consultare il personale	☐	☐	☐	☐
	(b) Gli account predefiniti non necessari vengono rimossi o disattivati prima dell'installazione di un sistema sulla rete?	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni di sistema e le impostazioni account ▪ Consultare il personale	☐	☐	☐	☐
2.1.1	Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, sono stati modificati tutti i valori predefiniti del fornitore wireless al momento dell'installazione, come segue:					
	(a) Sono state modificate le chiavi di cifratura predefinite al momento dell'installazione e vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede?	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Consultare il personale	☐	☐	☐	☐
	(b) Le stringhe di comunità SNMP predefinite sui dispositivi wireless sono state modificate al momento dell'installazione?	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Consultare il personale ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(c) Le password/passphrase predefinite sui punti di accesso sono state modificate al momento dell'installazione?	▪ Analizzare le politiche e le procedure ▪ Consultare il personale ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(d) Il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless?	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(e) Sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili?	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
2.2.2	(a) Sono abilitati solo i servizi, protocolli, daemon ecc. necessari come richiesto per la funzione del sistema (sono disabilitati i servizi e protocolli che non sono strettamente necessari per eseguire la funzione specifica di un dispositivo)?	▪ Analizzare gli standard di configurazione ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(b) Tutti i servizi, i daemon o i protocolli non sicuri attivi sono giustificati a fronte di standard di configurazione documentati?	▪ Analizzare gli standard di configurazione ▪ Consultare il personale ▪ Esaminare le impostazioni di configurazione ▪ Confrontare i servizi attivati ecc. in base alle giustificazioni documentate	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
2.2.3	Sono state documentate e implementate le funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuri? ***Nota:*** *laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.*	▪ Analizzare gli standard di configurazione ▪ Esaminare le impostazioni di configurazione	☐	☐	☐	☐
2.2.4	(a) Gli amministratori di sistema e/o il personale che si occupa della configurazione dei componenti di sistema conoscono in modo approfondito le impostazioni dei parametri di sicurezza per i componenti di sistema in questione?	▪ Consultare il personale	☐	☐	☐	☐
	(b) Le impostazioni dei parametri di sicurezza comuni del sistema sono comprese negli standard di configurazione del sistema?	▪ Analizzare gli standard di configurazione del sistema	☐	☐	☐	☐
	(c) Le impostazioni dei parametri di sicurezza sono impostate correttamente sui componenti di sistema?	▪ Esaminare i componenti di sistema ▪ Esaminare le impostazioni dei parametri di sicurezza ▪ Confrontare le impostazioni degli standard di configurazione del sistema	☐	☐	☐	☐
2.2.5	(a) È stata rimossa tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati?	▪ Esaminare i parametri di sicurezza sui componenti di sistema	☐	☐	☐	☐
	(b) Tutte le funzioni abilitate sono documentate e supportano una configurazione sicura?	▪ Analizzare la documentazione ▪ Esaminare i parametri di sicurezza sui componenti di sistema	☐	☐	☐	☐
	(c) Sui componenti di sistema sono presenti solo funzionalità documentate?	▪ Analizzare la documentazione ▪ Esaminare i parametri di sicurezza sui componenti di sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
2.3	È stata eseguita la cifratura dell'accesso amministrativo non da console come segue: ***Nota*: *laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.***					
	(a) È stata eseguita la cifratura di tutto l'accesso amministrativo non da console con crittografia avanzata? Viene richiamato un sistema di cifratura avanzata prima della richiesta della password dell'amministratore?	▪ Esaminare i componenti di sistema ▪ Esaminare le configurazioni del sistema ▪ Osservare un accesso amministratore	☐	☐	☐	☐
	(b) I servizi di sistema e i file dei parametri sono configurati in modo da impedire l'uso di Telnet e di altri comandi di accesso remoto non sicuri?	▪ Esaminare i componenti di sistema ▪ Esaminare servizi e file	☐	☐	☐	☐
	(c) L'accesso amministratore alle interfacce di gestione basate su Web è cifrato con un metodo di crittografia avanzata?	▪ Esaminare i componenti di sistema ▪ Osservare un accesso amministratore	☐	☐	☐	☐
	(d) Per la tecnologia in uso, viene implementata una crittografia avanzata in conformità alle migliori pratiche di settore e/o alle raccomandazioni del fornitore?	▪ Esaminare i componenti di sistema ▪ Analizzare la documentazione del fornitore ▪ Consultare il personale	☐	☐	☐	☐

Protezione dei dati dei titolari di carta

Requisito 3 - Proteggere i dati dei titolari di carta memorizzati

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
3.2	(c) I dati sensibili di autenticazione vengono eliminati o resi non recuperabili dopo il completamento del processo di autorizzazione?	▪ Analizzare le politiche e le procedure ▪ Esaminare le configurazioni del sistema ▪ Esaminare i processi di eliminazione	☐	☐	☐	☐
	(d) Tutti i sistemi aderiscono ai seguenti requisiti relativi alla non memorizzazione di dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati)?					
3.2.2	Il codice o il valore di verifica della carta (numero di tre o quattro cifre impresso sulla parte anteriore o sul retro di una carta di pagamento) non viene memorizzato dopo l'autorizzazione?	▪ Esaminare le origini dei dati tra cui: • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database	☐	☐	☐	☐
3.2.3	Il numero di identificazione personale (PIN) o il blocco PIN cifrato non viene memorizzato dopo l'autorizzazione?	▪ Esaminare le origini dei dati tra cui: • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
3.3	Il PAN completo viene mascherato quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) per renderlo visibile solo al personale autorizzato? ***Nota:*** *questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati dei titolari di carta, ad esempio requisiti legali o del marchio di carta di pagamento per ricevute di punti di vendita (POS).*	▪ Analizzare le politiche e le procedure ▪ Analizzare i ruoli che hanno la necessità di accedere alle visualizzazioni del PAN completo ▪ Esaminare le configurazioni del sistema ▪ Osservare le visualizzazioni del PAN	☐	☐	☐	☐

Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
4.1	(a) I protocolli di sicurezza e di crittografia avanzata sono stati utilizzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche e aperte? ***Nota:*** *laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.* *Esempi di reti pubbliche e aperte includono, senza limitazioni: Internet, tecnologie wireless, (compresi 802.11 e Bluetooth), tecnologie cellulari (ad es. le comunicazioni Global System for Mobile, GSM), CDMA (Code Division Multiple Access) e GPRS (General Packet Radio Service).*	▪ Analizzare gli standard documentati ▪ Analizzare le politiche e le procedure ▪ Analizzare tutte località in cui si trasmettono o ricevono i dati dei titolari di carta ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(b) (b) Vengono accettati solo certificati e/o chiavi affidabili?	▪ Osservare le trasmissioni in ingresso e in uscita ▪ Esaminare le chiavi e i certificati	☐	☐	☐	☐
	(c) Sono implementati protocolli di sicurezza per utilizzare solo configurazioni sicure e non supportare versioni o configurazioni non sicure?	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(d) Viene implementato il livello di crittografia corretto per la metodologia in uso (controllare i suggerimenti/le migliori pratiche del fornitore)?	▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(e) Per le implementazioni TLS, è abilitato TLS durante la trasmissione o la ricezione dei dati dei titolari di carta? *Ad esempio, per le implementazioni basate su browser:* • *"HTTPS" viene visualizzato come protocollo dell'URL del browser;* • *i dati dei titolari di carta vengono richiesti solo se "HTTPS" viene visualizzato come parte dell'URL.*	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
4.1.1	Le migliori pratiche di settore sono state utilizzate per implementare la cifratura avanzata per l'autenticazione e la trasmissione per le reti wireless che trasmettono i dati dei titolari di carta o connesse all'ambiente dei dati dei titolari di carta?	▪ Analizzare gli standard documentati ▪ Analizzare le reti wireless ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐
4.2	(b) Sono in atto politiche in cui viene indicato che i PAN non protetti non si devono inviare mediante tecnologie di messaggistica degli utenti finali?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐

Utilizzare un programma per la gestione delle vulnerabilità

Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
5.1	È stato installato un software antivirus su tutti i sistemi comunemente colpiti da software dannoso?	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
5.1.1	Tutti i programmi antivirus sono in grado di rilevare, rimuovere e proteggere da tutti i tipi conosciuti di software dannoso (ad esempio virus, cavalli di Troia, worm, spyware, adware e rootkit)?	▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
5.1.2	Vengono eseguite valutazioni periodiche per identificare e valutare l'evoluzione delle minacce malware e confermare se i sistemi considerati in genere non colpiti dal software dannoso continuano a essere sicuri?	▪ Consultare il personale	☐	☐	☐	☐
5.2	Tutti i meccanismi antivirus sono mantenuti come segue:					
	(a) Il software antivirus e le definizioni sono aggiornati?	▪ Esaminare le politiche e le procedure ▪ Esaminare le configurazioni antivirus, inclusa l'installazione principale ▪ Esaminare i componenti di sistema	☐	☐	☐	☐
	(b) Sono attivati e vengono eseguiti aggiornamenti automatici e scansioni periodiche?	▪ Esaminare le configurazioni antivirus, inclusa l'installazione principale ▪ Esaminare i componenti di sistema	☐	☐	☐	☐
	(c) Tutti i meccanismi antivirus generano log di audit e, questi log sono conservati in base al Requisito 10.7 PCI DSS?	▪ Esaminare le configurazioni antivirus ▪ Analizzare i processi di conservazione dei log	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
5.3	Tutti i meccanismi antivirus sono: ▪ Attivamente in esecuzione? ▪ Non disattivabili o modificabili dagli utenti? ***Nota:*** *è possibile disattivare temporaneamente le soluzioni antivirus solo in caso di esigenza tecnica legittima, come autorizzato dalla direzione per ogni singolo caso. Se è necessario disattivare la protezione antivirus per un motivo specifico, è opportuno essere autorizzati formalmente. Potrebbe essere necessario implementare ulteriori misure di sicurezza per il periodo di tempo in cui la protezione antivirus non è attiva.*	▪ Esaminare le configurazioni antivirus ▪ Esaminare i componenti di sistema ▪ Osservare i processi ▪ Consultare il personale	☐	☐	☐	☐

Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
6.1	È presente un processo per individuare vulnerabilità alla sicurezza, incluso quanto segue: ▪ Utilizzo di fonti esterne attendibili di informazioni sulle vulnerabilità? ▪ Assegnazione di una classificazione dei rischi alle vulnerabilità che include l'identificazione di tutte le vulnerabilità ad "alto rischio" e "critiche"? ***Nota**: le classificazioni dei rischi devono essere basate sulle migliori pratiche di settore nonché sulla valutazione del potenziale impatto. Ad esempio, i criteri per la classificazione delle vulnerabilità possono tenere in considerazione il punteggio base CVSS e/o la classificazione del fornitore e/o il tipo di sistemi interessati.* *I metodi per la valutazione delle vulnerabilità e l'assegnazione delle valutazioni dei rischi variano in base all'ambiente aziendale e alla strategia di valutazione dei rischi. Le classificazioni dei rischi devono almeno identificare tutte le vulnerabilità ad "alto rischio" per l'ambiente. Oltre alla classificazione dei rischi, le vulnerabilità possono essere considerate "critiche" se rappresentano una minaccia imminente per l'ambiente, influiscono sui sistemi critici e/o comportano una potenziale compromissione se non risolte. Esempi di sistemi critici includono sistemi di sicurezza, dispositivi e sistemi rivolti al pubblico, database e altri sistemi che memorizzano, elaborano o trasmettono i dati dei titolari di carta.*	▪ Analizzare le politiche e le procedure ▪ Consultare il personale ▪ Osservare i processi	☐	☐	☐	☐
6.2	(a) Tutti i componenti di sistema e il software sono protetti dalle vulnerabilità note mediante l'installazione delle patch di sicurezza dei fornitori?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(b) Sono state installate patch di protezione critiche entro un mese dal relativo rilascio? ***Nota**: le patch di sicurezza critiche vanno identificate in conformità al processo di classificazione dei rischi definito nel Requisito 6.1.*	▪ Analizzare le politiche e le procedure ▪ Esaminare i componenti di sistema ▪ Confrontare elenco delle patch di sicurezza installate con gli elenchi delle ultime patch del fornitore	☐	☐	☐	☐

Implementazione di rigide misure di controllo dell'accesso

Requisito 7 - Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
7.1	L'accesso ai componenti di sistema e ai dati di titolari di carta è limitato solo alle persone per le cui mansioni è realmente necessario, come segue:					
7.1.2	L'accesso agli ID utente con privilegi è limitato come segue: ▪ Alla quantità minima necessaria per le responsabilità di ruolo? ▪ Assegnato solo a ruoli che necessitano specificatamente tale accesso privilegiato?	▪ Esaminare la politica scritta di controllo dell'accesso ▪ Consultare il personale ▪ Consultare i membri del management ▪ Analizzare gli ID utente con privilegi	☐	☐	☐	☐
7.1.3	L'accesso viene assegnato in base alla classificazione e alla funzione del singolo ruolo del personale?	▪ Esaminare la politica scritta di controllo dell'accesso ▪ Consultare i membri del management ▪ Analizzare gli ID utente	☐	☐	☐	☐

*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?	▪ Analizzare le procedure delle password ▪ Consultare il personale	☐	☐	☐	☐
8.1.3	L'accesso per gli utenti non attivi viene disattivato o rimosso immediatamente?	▪ Analizzare le procedure delle password ▪ Esaminare gli utenti account non attivi ▪ Analizzare gli elenchi di accesso attuali ▪ Osservare i dispositivi di autenticazione fisici	☐	☐	☐	☐
8.2	Oltre ad assegnare un ID univoco, viene adottato uno o più dei seguenti metodi per autenticare tutti gli utenti? ▪ 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.	▪ Analizzare le procedure delle password ▪ Osservare i processi di autenticazione	☐	☐	☐	☐
8.2.3	(a) I parametri delle password utente vengono configurati per richiedere che password/passphrase soddisfino i seguenti requisiti? • 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.	▪ Esaminare le impostazioni di configurazione del sistema per verificare i parametri delle password	☐	☐	☐	☐

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: ▪ 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.	▪ Analizzare le politiche e le procedure ▪ Esaminare gli elenchi di ID utente ▪ Consultare il personale	☐	☐	☐	☐

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
9.1	I controlli dell'accesso alle strutture appropriati sono utilizzati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta?	▪ Osservare i controlli di accesso fisici ▪ Osservare il personale	☐	☐	☐	☐
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	☐	☐	☐	☐
9.6	(a) La distribuzione interna ed esterna di qualsiasi tipo di supporto è rigorosamente controllata?	▪ Analizzare le politiche e le procedure per la distribuzione dei supporti	☐	☐	☐	☐
	(b) I controlli devono includere quanto segue:					
9.6.1	Il supporto è classificato in modo da poter determinare la sensibilità dei dati?	▪ Analizzare le politiche e le procedure per la classificazione dei supporti ▪ Consultare il personale di sicurezza	☐	☐	☐	☐
9.6.2	Il supporto viene inviato tramite un corriere affidabile o un altro metodo di consegna che può essere adeguatamente monitorato?	▪ Consultare il personale ▪ Esaminare i registri di controllo e la documentazione della distribuzione dei supporti	☐	☐	☐	☐
9.6.3	L'approvazione del management viene concessa prima dello spostamento dei supporti (soprattutto quando i supporti vengono distribuiti agli individui)?	▪ Consultare il personale ▪ Esaminare i registri di controllo e la documentazione della distribuzione dei supporti	☐	☐	☐	☐
9.7	Sono in atto controlli adeguati per la memorizzazione e l'accesso ai supporti?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
9.8	(a) 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:					

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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?	▪ 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	☐	☐	☐	☐

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.)*			
			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	☐	☐	☐	☐
12.3	Sono state sviluppate politiche che regolano l'uso per tecnologie critiche per definire l'uso corretto di queste tecnologie? Tali politiche richiedono quanto segue: ***Nota:*** *esempi di tecnologie critiche comprendono, senza limitazioni, accesso remoto e tecnologie wireless, laptop, tablet, supporti elettronici rimovibili, uso della posta elettronica e di Internet.*					
12.3.1	Approvazione esplicita delle parti autorizzate per l'uso delle tecnologie?	▪ Analizzare le politiche di utilizzo ▪ Consultare il personale responsabile	☐	☐	☐	☐
12.3.3	Un elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso?	▪ Analizzare le politiche di utilizzo ▪ Consultare il personale responsabile	☐	☐	☐	☐
12.3.5	Usi accettabili delle tecnologie?	▪ Analizzare le politiche di utilizzo ▪ Consultare il personale responsabile	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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	☐	☐	☐	☐
12.5	(b) Le seguenti responsabilità per la gestione della sicurezza delle informazioni sono state assegnate a una singola persona o a un team?					
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	☐	☐	☐	☐
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	☐	☐	☐	☐
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	☐	☐	☐	☐
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	☐	☐	☐	☐

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

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
A2.1	*Per i terminali POS POI (e i punti di terminazione SSL/TLS a cui si connettono) che utilizzano SSL e/o TLS iniziale:* • È confermato che i dispositivi non sono soggetti a eventuali exploit noti per SSL/TLS iniziale *O:* • È in atto un piano formale di migrazione e riduzione dei rischi in base al Requisito A2.2?	▪ Analizzare la documentazione (ad esempio, documentazione del fornitore, dettagli di configurazione del sistema/della rete, ecc.) che verifica che i dispositivi POS POI non siano soggetti a eventuali exploit noti per SSL/TLS iniziale	☐	☐	☐	☐
A2.2	È in atto un piano formale di migrazione e di riduzione dei rischi per tutte le implementazioni che utilizzano SSL e/o TLS iniziale (diverso da quanto consentito in A2.1), che include: ▪ descrizione dell'utilizzo, inclusi il tipo di dati trasmessi, i tipi e il numero di sistemi che utilizzano e/o supportano SSL/TLS iniziale come tipo di ambiente; ▪ risultati della valutazione dei rischi e controlli per la riduzione dei rischi in atto; ▪ descrizione dei processi per ricercare eventuali nuove vulnerabilità associate a SSL/TLS iniziale; ▪ descrizione dei processi di controllo delle modifiche implementati per accertarsi che SSL/TLS iniziale non venga implementato nei nuovi ambienti; ▪ panoramica del piano del progetto di migrazione inclusa la data di completamento della migrazione prevista non oltre il 30 giugno 2018?	▪ Analizzare il piano documentato di migrazione e di riduzione dei rischi	☐	☐	☐	☐

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:	
3.4	I dati dei titolari di carta non vengono mai archiviati in formato elettronico

Sezione 3 - Dettagli su convalida e attestato

Parte 3. Convalida PCI DSS

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

In base ai risultati documentati nel questionario SAQ C-VT 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 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 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.*
☐	**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 C-VT, 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 verificato con il fornitore dell'applicazione di pagamento che il mio sistema di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
☐	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 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.
☐	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, 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	
1	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta	☐	☐	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	☐	☐	
3	Proteggere i dati dei titolari di carta memorizzati	☐	☐	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	☐	☐	
5	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus	☐	☐	
6	Sviluppare e gestire sistemi e applicazioni protette	☐	☐	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	☐	☐	
8	Individuare e autenticare l'accesso ai componenti di sistema	☐	☐	
9	Limitare l'accesso fisico ai dati dei titolari di carta	☐	☐	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	☐	☐	
Appendice A2	Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale	☐	☐	

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