

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

Questionario di autovalutazione C e Attestato di conformità

**Esercenti con sistemi di pagamento
connessi a Internet-
Nessuna memorizzazione elettronica dei
dati dei titolari di carta**

Per l'uso con PCI DSS versione 3.2

Aprile 2016

Modifiche del documento

Data	Versione PCI DSS	Revision e SAQ	Descrizione
Ottobre 2008	1.2		Allineare il contenuto con il nuovo standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.
Ottobre 2010	2.0		Allineare il contenuto ai nuovi requisiti e procedure di test PCI DSS v2.0.
Febbraio 2014	3.0		Allineare il contenuto con i requisiti PCI DSS v3.0 e le procedure di test e incorporare ulteriori opzioni di risposta.
Aprile 2015	3.1		Aggiornato per allinearli a PCI DSS v3.1. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.0 alla 3.1</i> .
Luglio 2015	3.1	1.1	Aggiornato per rimuovere i riferimenti alle “migliori pratiche” prima del 30 giugno 2015.
Aprile 2016	3.2	1.0	Aggiornato per allinearli a PCI DSS v3.2. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.1 alla 3.2</i> .

Sommario

Modifiche del documento	i
Operazioni preliminari	iii
Passaggi per il completamento dell'autovalutazione PCI DSS	iii
Comprensione del questionario di autovalutazione	iv
<i>Test previsti</i>	<i>iv</i>
Completamento del questionario di autovalutazione	v
Guida per la non applicabilità di determinati requisiti specifici	v
Eccezione legale	v
Sezione 1 - Informazioni sulla valutazione	1
Sezione 2 - Questionario di autovalutazione C	4
Sviluppo e gestione di sistemi e reti sicure	4
<i>Requisito 1 - Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta</i>	<i>4</i>
<i>Requisito 2 - Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione</i>	<i>6</i>
Protezione dei dati dei titolari di carta	12
<i>Requisito 3 - Proteggere i dati dei titolari di carta memorizzati</i>	<i>12</i>
<i>Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche</i>	<i>14</i>
Utilizzare un programma per la gestione delle vulnerabilità	16
<i>Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus</i>	<i>16</i>
<i>Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette</i>	<i>18</i>
Implementazione di rigide misure di controllo dell'accesso	20
<i>Requisito 7 - Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario</i>	<i>20</i>
<i>Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema</i>	<i>21</i>
Monitoraggio e test delle reti regolari	30
<i>Requisito 10 - Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta</i> ..	<i>30</i>
<i>Requisito 11 - Eseguire regolarmente test dei sistemi e processi di protezione</i>	<i>33</i>
Gestire una politica di sicurezza delle informazioni	39
<i>Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale</i>	<i>39</i>
Appendice A - Requisiti PCI DSS aggiuntivi	43
<i>Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i>	<i>43</i>
<i>Appendice A2 - Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale</i>	<i>43</i>
<i>Appendice A3 - Convalida aggiuntiva delle entità designate (DESV)</i>	<i>44</i>
Appendice B - Foglio di lavoro - Controlli compensativi	45
Appendice C - Spiegazione di non applicabilità	46
Sezione 3 - Dettagli su convalida e attestato	47

Operazioni preliminari

Il questionario SAQ C è stato sviluppato per rispondere ai requisiti applicabili ad esercenti i cui sistemi di pagamento (ad esempio, sistemi POS) sono connessi a Internet (ad esempio tramite DSL, modem via cavo, ecc.).

Gli esercenti SAQ C elaborano i dati dei titolari di carta mediante sistemi POS o altri sistemi di pagamento connessi a Internet, non memorizzano tali dati su un computer e possono essere società di e-commerce con punti vendita reali (carta presente) o società di vendita tramite posta elettronica/telefono (carta non presente).

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

- La società dispone di un sistema di applicazione di pagamento e di una connessione Internet sul medesimo dispositivo e/o sulla stessa rete locale (LAN).
- L'applicazione di pagamento/dispositivo Internet non è collegato ad altri sistemi all'interno dell'ambiente (ciò può essere ottenuto mediante la segmentazione di rete per isolare l'applicazione di pagamento/dispositivo Internet da tutti gli altri sistemi).
- La posizione fisica dell'ambiente POS non è connessa ad altre sedi o posizioni e la rete LAN è destinata solo a una posizione singola.
- 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 quanto definito nei criteri di idoneità esposti in precedenza. Qualora siano presenti requisiti PCI DSS applicabili al proprio ambiente che non sono coperti dal presente questionario di autovalutazione, ciò potrebbe indicare che questo questionario non è adatto al proprio ambiente. Inoltre, è comunque necessario soddisfare tutti i requisiti PCI DSS applicabili per garantire la conformità agli standard PCI DSS.

Passaggi per il completamento dell'autovalutazione PCI DSS

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

Comprensione del questionario di autovalutazione

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

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

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

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

Test previsti

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

Completamento del questionario di autovalutazione

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

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

Risposta	Quando utilizzare questa risposta:
Sì	Il test previsto è stato eseguito e tutti gli elementi del requisito sono stati soddisfatti come indicato.
Sì con CCW (Foglio di lavoro - Controllo compensativo)	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 <i>Guida per la non applicabilità di determinati requisiti specifici</i> 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 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). Tenere presente che occorre comunque fornire una risposta al requisito 11.1 (uso di processi per identificare punti di accesso wireless non autorizzati) anche se la propria rete non prevede la tecnologia wireless, perché il processo rileva eventuali intrusioni o dispositivi non autorizzati che possono essere stati aggiunti a vostra insaputa.

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

Eccezione legale

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

Sezione 1 - Informazioni sulla valutazione

Istruzioni per l'invio

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

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

Parte 1a. Informazioni sull'organizzazione dell'esercente

Ragione sociale:		DBA (doing business as):	
Nome referente:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP:
URL:			

Parte 1b. Informazioni sull'azienda qualificata per la valutazione (se applicabile)

Ragione sociale:			
Nome referente QSA principale:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP:
URL:			

Parte 2. Riepilogo esecutivo

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

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

Quali tipi di canali di pagamento offre l'azienda?

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

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

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

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

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

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

Parte 2c. Sedi

Elenco dei tipi di struttura 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)
<i>Esempio: punti vendita</i>	3	<i>Boston, MA, Stati Uniti</i>

Parte 2d. Applicazione di pagamento

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

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

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

Parte 2e. Descrizione dell'ambiente

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

Ad esempio:

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

L'azienda utilizza la segmentazione di rete per definire l'ambito del proprio ambiente PCI DSS? (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:	<input type="checkbox"/> Sì <input type="checkbox"/> 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.)?	<input type="checkbox"/> Sì <input type="checkbox"/> 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

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

<input type="checkbox"/>	L'esercente dispone di un sistema di applicazione di pagamento e di una connessione Internet sul medesimo dispositivo e/o sulla stessa rete locale (LAN).
<input type="checkbox"/>	Il dispositivo con il sistema di pagamento/Internet non è connesso ad altri sistemi all'interno dell'ambiente dell'esercente.
<input type="checkbox"/>	La posizione fisica dell'ambiente POS non è connessa ad altre sedi o posizioni e la rete LAN è destinata solo a una posizione singola.
<input type="checkbox"/>	L'esercente non memorizza dati dei titolari di carta in formato elettronico.
<input type="checkbox"/>	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

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?	<ul style="list-style-type: none"> Analizzare gli standard di configurazione di firewall e router Esaminare le configurazioni di firewall e router 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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".	<ul style="list-style-type: none"> Analizzare gli standard di configurazione di firewall e router Esaminare le configurazioni di firewall e router 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Analizzare gli standard di configurazione di firewall e router Esaminare le configurazioni di firewall e router 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Sono consentite nella rete solo le connessioni già stabilite?	▪ Esaminare le configurazioni di firewall e router	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
	(c) Le password/passphrase predefinite sui punti di accesso sono state modificate al momento dell'installazione?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Consultare il personale Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Analizzare la documentazione del fornitore Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(e) Sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Analizzare la documentazione del fornitore Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2	(a) Sono stati sviluppati standard di configurazione per tutti i componenti di sistema e sono coerenti con gli standard di System Hardening che sono accettati dal settore? <i>Fonti di standard di System Hardening accettati dal settore possono comprendere, senza limitazione, enti quali SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) e Center for Internet Security (CIS).</i>	<ul style="list-style-type: none"> Analizzare gli standard di configurazione del sistema Analizzare gli standard di hardening accettati dal settore Analizzare le politiche e le procedure Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sono aggiornati gli standard di configurazione del sistema in caso di identificazione di nuovi problemi di vulnerabilità, secondo quanto definito al Requisito 6.1?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Quando si configurano nuovi sistemi, vengono applicati gli standard di configurazione del sistema?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Si	Si con CCW	No	N/A
(d) Gli standard di configurazione del sistema comprendono quanto segue: <ul style="list-style-type: none"> • Modifica di tutti i valori predefiniti del fornitore ed eliminazione di account predefiniti non necessari? • Implementazione di una sola funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi? • Abilitazione di servizi, protocolli, daemon, ecc. necessari, come richiesto per la funzione del sistema? • Implementazione di funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuro? • Configurazione di parametri di sicurezza del sistema per evitare un uso improprio? • Rimozione di tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati? 	<ul style="list-style-type: none"> ▪ Analizzare gli standard di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1 (a) È implementata una sola funzione primaria per server, per evitare la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi? <i>Ad esempio, server Web, database server e DNS devono essere implementati su server separati.</i>	<ul style="list-style-type: none"> ▪ Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) In caso di utilizzo di tecnologie di virtualizzazione, viene implementata una sola funzione primaria per dispositivo o componente di sistema virtuale?	<ul style="list-style-type: none"> ▪ Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
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)?	<ul style="list-style-type: none"> Analizzare gli standard di configurazione Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Tutti i servizi, i daemon o i protocolli non sicuri attivi sono giustificati a fronte di standard di configurazione documentati?	<ul style="list-style-type: none"> Analizzare gli standard di configurazione Consultare il personale Esaminare le impostazioni di configurazione Confrontare i servizi attivati ecc. in base alle giustificazioni documentate 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	<p>Sono state documentate e implementate le funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuri?</p> <p>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</p>	<ul style="list-style-type: none"> Analizzare gli standard di configurazione Esaminare le impostazioni di configurazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Le impostazioni dei parametri di sicurezza comuni del sistema sono comprese negli standard di configurazione del sistema?	<ul style="list-style-type: none"> Analizzare gli standard di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Le impostazioni dei parametri di sicurezza sono impostate correttamente sui componenti di sistema?	<ul style="list-style-type: none"> Esaminare i componenti di sistema Esaminare le impostazioni dei parametri di sicurezza Confrontare le impostazioni degli standard di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
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?	<ul style="list-style-type: none"> Esaminare i parametri di sicurezza sui componenti di sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Tutte le funzioni abilitate sono documentate e supportano una configurazione sicura?	<ul style="list-style-type: none"> Analizzare la documentazione Esaminare i parametri di sicurezza sui componenti di sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Sui componenti di sistema sono presenti solo funzionalità documentate?	<ul style="list-style-type: none"> Analizzare la documentazione Esaminare i parametri di sicurezza sui componenti di sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3	<p>È stata eseguita la cifratura dell'accesso amministrativo non da console come segue:</p> <p>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</p>					
	(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?	<ul style="list-style-type: none"> Esaminare i componenti di sistema Esaminare le configurazioni del sistema Osservare un accesso amministratore 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> Esaminare i componenti di sistema Esaminare servizi e file 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) L'accesso amministratore alle interfacce di gestione basate su Web è cifrato con un metodo di crittografia avanzata?	<ul style="list-style-type: none"> Esaminare i componenti di sistema Osservare un accesso amministratore 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Per la tecnologia in uso, viene implementata una crittografia avanzata in conformità alle migliori pratiche di settore e/o alle raccomandazioni del fornitore?	<ul style="list-style-type: none"> Esaminare i componenti di sistema Analizzare la documentazione del fornitore Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
2.5	Le politiche di sicurezza e le procedure operative per la gestione delle impostazioni predefinite del fornitore e dei parametri di sicurezza sono: <ul style="list-style-type: none"> ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte? 	<ul style="list-style-type: none"> ▪ Analizzare le politiche di sicurezza e le procedure operative ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Esaminare le configurazioni del sistema ▪ Esaminare i processi di eliminazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Tutti i sistemi aderiscono ai seguenti requisiti relativi alla non memorizzazione di dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati)?					
3.2.1	<p>L'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, contenuto in un chip o in altro luogo) non viene memorizzato dopo l'autorizzazione?</p> <p><i>Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati della striscia magnetica.</i></p> <p>Nota: nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</p> <ul style="list-style-type: none"> • Nome del titolare della carta • PAN (Primary Account Number) • Data di scadenza • Codice di servizio <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</i></p>	<ul style="list-style-type: none"> ▪ Esaminare le origini dei dati tra cui: <ul style="list-style-type: none"> • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
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?	<ul style="list-style-type: none"> ▪ Esaminare le origini dei dati tra cui: <ul style="list-style-type: none"> • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Il numero di identificazione personale (PIN) o il blocco PIN cifrato non viene memorizzato dopo l'autorizzazione?	<ul style="list-style-type: none"> ▪ Esaminare le origini dei dati tra cui: <ul style="list-style-type: none"> • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3	<p>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?</p> <p>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).</p>	<ul style="list-style-type: none"> ▪ 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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? <i>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</i> <i>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).</i>	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Vengono accettati solo certificati e/o chiavi affidabili?	<ul style="list-style-type: none"> Osservare le trasmissioni in ingresso e in uscita Esaminare le chiavi e i certificati 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Sono implementati protocolli di sicurezza per utilizzare solo configurazioni sicure e non supportare versioni o configurazioni non sicure?	<ul style="list-style-type: none"> Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Viene implementato il livello di crittografia corretto per la metodologia in uso (controllare i suggerimenti, le pratiche consigliate del fornitore)?	<ul style="list-style-type: none"> Analizzare la documentazione del fornitore Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) Per le implementazioni TLS, è abilitato TLS durante la trasmissione o la ricezione dei dati dei titolari di carta? <i>Ad esempio, per le implementazioni basate su browser:</i> <ul style="list-style-type: none"> "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. 	<ul style="list-style-type: none"> Esaminare le configurazioni del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
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? _____	<ul style="list-style-type: none"> ▪ Analizzare gli standard documentati ▪ Analizzare le reti wireless ▪ Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(b) Sono presenti politiche in cui si indica che i PAN non protetti non devono essere inviati mediante tecnologie di messaggistica degli utenti finali?	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.)			
		Si	Si con CCW	No	N/A
5.1	È stato installato un software antivirus su tutti i sistemi comunemente colpiti da software dannoso?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Tutti i meccanismi antivirus sono mantenuti come segue:				
(a)	Il software antivirus e le definizioni sono aggiornati?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b)	Sono attivati e vengono eseguiti aggiornamenti automatici e scansioni periodiche?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c)	Tutti i meccanismi antivirus generano log di audit e, questi log sono conservati in base al Requisito 10.7 PCI DSS?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
5.3	<p>Tutti i meccanismi antivirus sono:</p> <ul style="list-style-type: none"> ▪ Attivamente in esecuzione? ▪ Non disattivabili o modificabili dagli utenti? <p><i>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.</i></p>	<ul style="list-style-type: none"> ▪ Esaminare le configurazioni antivirus ▪ Esaminare i componenti di sistema ▪ Osservare i processi ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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
<p>6.1 È presente un processo per individuare vulnerabilità alla sicurezza, incluso quanto segue:</p> <ul style="list-style-type: none"> ▪ 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"? <p>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.</p> <p><i>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.</i></p>	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Consultare il personale ▪ Osservare i processi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
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?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sono state installate patch di protezione critiche entro un mese dal relativo rilascio? <i>Nota: le patch di sicurezza critiche vanno identificate in conformità al processo di classificazione dei rischi definito nel Requisito 6.1.</i>	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.6	Al completamento di una modifica significativa, tutti i requisiti PCI DSS rilevanti sono implementati su tutte le reti e tutti i sistemi nuovi o modificati e la documentazione viene aggiornata come applicabile? <i>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</i>	<ul style="list-style-type: none"> Tenere traccia delle modifiche per aggiornare la documentazione di controllo Esaminare la documentazione di controllo delle modifiche Consultare il personale Osservare le reti o i sistemi interessati 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.)			
			Si	Si 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: <ul style="list-style-type: none"> Alla quantità minima necessaria per le responsabilità di ruolo? Assegnato solo a ruoli che necessitano specificatamente tale accesso privilegiato? 	<ul style="list-style-type: none"> Esaminare la politica scritta di controllo dell'accesso Consultare il personale Consultare i membri del management Analizzare gli ID utente con privilegi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	L'accesso viene assegnato in base alla classificazione e alla funzione del singolo ruolo del personale?	<ul style="list-style-type: none"> Esaminare la politica scritta di controllo dell'accesso Consultare i membri del management Analizzare gli ID utente 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Si con CCW	No	N/A
8.1	Sono state definite e applicate le politiche e le procedure per i controlli di gestione dell'identificazione dell'utente per utenti non consumatori e amministratori in tutti i componenti del sistema, come segue:					
8.1.1	A tutti gli utenti viene assegnato un ID univoco prima di consentire loro l'accesso a componenti del sistema o dati di titolari di carta?	<ul style="list-style-type: none"> Analizzare le procedure delle password Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.5	(a) Gli account utilizzati da terzi per accedere, fornire supporto o manutenzione ai componenti di sistema mediante accesso remoto sono abilitati solo durante il periodo di tempo necessario e disabilitati se non in uso?	<ul style="list-style-type: none"> Analizzare le procedure delle password Consultare il personale Osservare i processi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Gli account per l'accesso in remoto di terzi vengono monitorati durante l'uso?	<ul style="list-style-type: none"> Consultare il personale Osservare i processi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.6	(a) I tentativi di accesso ripetuti sono limitati bloccando l'ID utente dopo un massimo di sei tentativi?	<ul style="list-style-type: none"> Analizzare le procedure delle password Esaminare le impostazioni di configurazione del sistema 				
8.1.7	Una volta che un account utente è bloccato, la durata del blocco è impostata almeno su 30 minuti oppure fino a quando l'amministratore non abilita nuovamente l'ID utente?	<ul style="list-style-type: none"> Analizzare le procedure delle password Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.8	Se una sessione è inattiva per più di 15 minuti, agli utenti viene richiesto di effettuare nuovamente l'autenticazione (ad esempio immettere di nuovo la password) per riattivare il terminale o la sessione?	<ul style="list-style-type: none"> Analizzare le procedure delle password Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
8.2	<p>Oltre ad assegnare un ID univoco, viene adottato uno o più dei seguenti metodi per autenticare tutti gli utenti?</p> <ul style="list-style-type: none"> ▪ qualcosa che l'utente conosce, come una password o una passphrase; ▪ Qualcosa in possesso dell'utente, come un dispositivo token o una smart card ▪ qualcosa che l'utente è, come un elemento biometrico. 	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Osservare i processi di autenticazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.3	<p>(a) I parametri delle password utente vengono configurati per richiedere che password/passphrase soddisfino i seguenti requisiti?</p> <ul style="list-style-type: none"> • Lunghezza minima della password di 7 caratteri • Presenza di caratteri numerici e alfabetici <p>In alternativa, le password/passphrase devono presentare una complessità e solidità pari almeno ai parametri indicati sopra.</p>	<ul style="list-style-type: none"> ▪ Esaminare le impostazioni di configurazione del sistema per verificare i parametri delle password 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.4	<p>Le password/passphrase degli utenti vengono modificate almeno una volta ogni 90 giorni?</p>	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.5	<p>La nuova password/passphrase specificata deve essere diversa dalle ultime quattro password/passphrase utilizzate?</p>	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Componente di sistema campione ▪ Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.6	<p>Le password/passphrase sono impostate su un valore univoco per ciascun utente per il primo accesso e al ripristino e ogni utente modifica la propria password immediatamente dopo il primo accesso?</p>	<ul style="list-style-type: none"> ▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema ▪ Osservare il personale di sicurezza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	
8.3	<p>Tutto il singolo accesso amministrativo non da console e tutto l'accesso remoto al CDE vengono protetti mediante l'autenticazione a più fattori, nel modo seguente:</p> <p>Nota: <i>l'autenticazione a più fattori richiede l'utilizzo di almeno due dei tre metodi di autenticazione (fare riferimento al Requisito 8.2 PCI DSS per le descrizioni dei metodi di autenticazione). Utilizzare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a più fattori.</i></p>					
8.3.1	<p>È stata integrata l'autenticazione a più fattori per tutto l'accesso non da console al CDE per il personale con l'accesso amministrativo?</p> <p>Nota: <i>questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</i></p>	<ul style="list-style-type: none"> ▪ Esaminare le configurazioni del sistema ▪ Osservare l'accesso al CDE da parte dell'amministratore del personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3.2	<p>È stata integrata l'autenticazione a più fattori per tutto l'accesso remoto alla rete (sia utente che amministratore e incluso l'accesso di terzi per supporto o manutenzione) originato al di fuori della rete dall'entità?</p>	<ul style="list-style-type: none"> ▪ Esaminare le configurazioni del sistema ▪ Osservare la connessione del personale in remoto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4	<p>(a) Le procedure e le politiche di autenticazione vengono documentate e comunicate a tutti gli utenti?</p>	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Analizzare il metodo di distribuzione ▪ Consultare il personale ▪ Consultare gli utenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
	(b) Le procedure e le politiche di autenticazione includono quanto segue? <ul style="list-style-type: none"> • Istruzioni sulla selezione di credenziali di autenticazione avanzata • Istruzioni su come gli utenti dovrebbero proteggere le proprie credenziali di autenticazione • Istruzioni per non riutilizzare le password utilizzate precedentemente • Istruzioni su come gli utenti devono modificare le password in caso di sospetta compromissione delle password 	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione fornita agli utenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.5	Account e password di gruppo, condivisi o generici o altri metodi di autenticazione sono vietati come segue: <ul style="list-style-type: none"> ▪ Gli ID e gli account utente generici sono disabilitati o rimossi. ▪ Non esistono ID utente condivisi per le attività di amministrazione del sistema e per altre funzioni critiche. ▪ Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema. 	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure ▪ Esaminare gli elenchi di ID utente ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.8	Le politiche di sicurezza e le procedure operative per l'identificazione e l'autenticazione sono: <ul style="list-style-type: none"> ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte? 	<ul style="list-style-type: none"> ▪ Esaminare le politiche di sicurezza e le procedure operative ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Si 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?	<ul style="list-style-type: none"> Osservare i controlli di accesso fisici Osservare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.1	(a) Sono presenti videocamere o meccanismi di controllo dell'accesso (o entrambi) per monitorare gli accessi fisici ad aree sensibili? Nota: Per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree rivolte al pubblico in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Osservare i meccanismi di monitoraggio fisici Osservare le funzionalità di protezione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Le videocamere o meccanismi di controllo dell'accesso (o entrambi) sono protetti da manomissione o disabilitazione?	<ul style="list-style-type: none"> Osservare i processi Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) I dati raccolti dalle videocamere e/o dai meccanismi di controllo dell'accesso vengono analizzati e correlati con altri dati?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Consultare il personale di sicurezza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) I dati raccolti dalle videocamere e/o da altri meccanismi di controllo dell'accesso vengono memorizzati per almeno tre mesi, se non diversamente richiesto dalla legge?	<ul style="list-style-type: none"> Analizzare i processi di conservazione dei dati Osservare la memorizzazione dei dati Consultare il personale di sicurezza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.2	Sono stati adottati i controlli fisici e/o logici per limitare l'accesso ai connettori di rete pubblicamente accessibili? <i>Ad esempio, i connettori di rete che si trovano nelle aree pubbliche e nelle aree accessibili ai visitatori potrebbero essere disattivati e attivati solo quando l'accesso alla rete è autorizzato esplicitamente. In alternativa, è possibile implementare i processi per garantire che i visitatori siano scortati costantemente nelle aree con connettori di rete attivi.</i>	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Consultare il personale Osservare le posizioni 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
9.5	Tutti i supporti sono protetti fisicamente (inclusi, senza limitazione, computer, supporti elettronici rimovibili, ricevute cartacee, resoconti cartacei e fax)? <i>Ai fini del Requisito 9, per "supporti" si intendono tutti i supporti elettronici e cartacei contenenti dati di titolari di carta.</i>	<ul style="list-style-type: none"> Analizzare le politiche e le procedure per proteggere fisicamente i supporti Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6	(a) La distribuzione interna ed esterna di qualsiasi tipo di supporto è rigorosamente controllata?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure per la distribuzione dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I controlli devono includere quanto segue:					
9.6.1	Il supporto è classificato in modo da poter determinare la sensibilità dei dati?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure per la classificazione dei supporti Consultare il personale di sicurezza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	Il supporto viene inviato tramite un corriere affidabile o un altro metodo di consegna che può essere adeguatamente monitorato?	<ul style="list-style-type: none"> Consultare il personale Esaminare i registri di controllo e la documentazione della distribuzione dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	L'approvazione del management viene concessa prima dello spostamento dei supporti (soprattutto quando i supporti vengono distribuiti agli individui)?	<ul style="list-style-type: none"> Consultare il personale Esaminare i registri di controllo e la documentazione della distribuzione dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	Sono in atto controlli adeguati per la memorizzazione e l'accesso ai supporti?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure di distruzione periodica dei supporti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) La distruzione dei supporti avviene in base alle seguenti modalità:					
9.8.1	(a) I materiali cartacei sono stati distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo che non sia possibile ricostruire i dati dei titolari di carta?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure di distruzione periodica dei supporti Consultare il personale Osservare i processi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
	(b) I contenitori usati per conservare i materiali che contengono le informazioni da distruggere sono protetti per impedire l'accesso al contenuto?	<ul style="list-style-type: none"> Esaminare la sicurezza dei contenitori di conservazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	<p>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?</p> <p>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.</p>					
	(a) Le politiche e le procedure prevedono che venga conservato un elenco di tali dispositivi?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Le politiche e le procedure richiedono che i dispositivi siano sottoposti a un'ispezione periodica per controllare eventuali manomissioni o sostituzioni?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.1	<p>(a) L'elenco dei dispositivi include quanto segue?</p> <ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Esaminare l'elenco dei dispositivi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) L'elenco è accurato e aggiornato?	<ul style="list-style-type: none"> Osservare i dispositivi e le relative posizioni e confrontarli con l'elenco 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
	(c) L'elenco di dispositivi viene aggiornato quando i dispositivi vengono aggiunti, riposizionati, messi fuori uso ecc.?	<ul style="list-style-type: none"> Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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.	<ul style="list-style-type: none"> Consultare il personale Osservare i processi di ispezione e confrontare con processi definiti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Il personale è a conoscenza delle procedure per ispezionare i dispositivi?	<ul style="list-style-type: none"> Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Sì	Sì con CCW	No	N/A
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?				
(c)	<p>Il materiale formativo per il personale dei punti vendita include quanto segue?</p> <ul style="list-style-type: none"> • 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). 	<p>▪ Analizzare i materiali di formazione</p> <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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?	<p>▪ Consultare il personale presso le sedi POS</p> <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Monitoraggio e test delle reti regolari

Requisito 10 - Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
10.2	Sono stati implementati audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:					
10.2.2	Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	Tentativi di accesso logico non validi?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.5	Uso e modifiche dei meccanismi di identificazione e autenticazione (compresi, a titolo esemplificativo, creazione di nuovi account, incremento dei privilegi, ecc.) e tutte le modifiche, le aggiunte e le eliminazioni agli account dell'applicazione con privilegi root o di amministratore?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Vengono registrate le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:					
10.3.1	Identificazione utente?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	Tipo di evento?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
10.3.3	Data e ora?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.4	Indicazione di successo o fallimento?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.5	Origine dell'evento?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identità o nome del dato interessato, componente di sistema o risorsa?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	<p>I registri e gli eventi di sicurezza per tutti i componenti di sistema vengono analizzati al fine di identificare anomalie o attività sospette, come indicato di seguito?</p> <p>Nota: gli strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità al requisito 10.6.</p>					

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
10.6.1	(b) I seguenti registri ed eventi di sicurezza vengono analizzati almeno una volta al giorno, sia manualmente che attraverso strumenti di registro? <ul style="list-style-type: none"> • Tutti gli eventi di sicurezza. • Registri di tutti i componenti di sistema che memorizzano, elaborano o trasmettono CHD e/o SAD. • Registri di tutti i componenti di sistema critici. • Registri di tutti i server e componenti di sistema che eseguono funzioni di sicurezza (ad esempio, firewall, sistemi di rilevamento intrusioni/sistemi di prevenzione intrusioni IDS/IPS, server di autenticazione, server di ridirezionamento e-commerce). 	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure di sicurezza ▪ Osservare i processi ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.2	(b) I registri e tutti gli altri componenti di sistema vengono rivisti periodicamente, manualmente o tramite strumenti di registro, in base alle politiche e alla strategia di gestione del rischio dell'azienda?	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure di sicurezza ▪ Analizzare la documentazione di valutazione dei rischi ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.3	(b) Viene eseguito il follow-up di eccezioni e anomalie individuate durante il processo di revisione?	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure di sicurezza ▪ Osservare i processi ▪ Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7	(b) I log di audit vengono conservati per almeno un anno?	<ul style="list-style-type: none"> ▪ Analizzare le politiche e le procedure di sicurezza ▪ Consultare il personale ▪ Esaminare i log di audit 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Sono immediatamente disponibili per l'analisi almeno i log degli ultimi tre mesi?	<ul style="list-style-type: none"> ▪ Consultare il personale ▪ Osservare i processi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requisito 11 - Eseguire regolarmente test dei sistemi e processi di protezione

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Si	Si con CCW	No	N/A
11.1 (a) I processi per il rilevamento e l'identificazione dei punti di accesso wireless autorizzati e non autorizzati vengono implementati almeno a cadenza trimestrale? Nota: i metodi che si possono utilizzare nel processo comprendono, senza limitazioni, scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless. Qualunque sia il metodo adottato, questo deve essere in grado di rilevare e identificare qualsiasi dispositivo non autorizzato.	<ul style="list-style-type: none"> Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) La metodologia rileva e identifica ogni punto di accesso wireless non autorizzato, compreso, come minimo, quanto segue? <ul style="list-style-type: none"> Schede WLAN inserite nei componenti di sistema Dispositivi portatili o mobili collegati ai componenti di sistema per creare un punto di accesso wireless (ad esempio, con USB, ecc.) Dispositivi wireless collegati a una porta o a un dispositivo di rete 	<ul style="list-style-type: none"> Valutare la metodologia 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) La scansione wireless finalizzata a identificare i punti di accesso wireless autorizzati e non autorizzati viene eseguita con cadenza trimestrale per tutte le strutture e i componenti di sistema?	<ul style="list-style-type: none"> Esaminare l'output delle scansioni wireless recenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) In caso di utilizzo del monitoraggio automatico (ad esempio, IDS/IPS wireless, NAC, ecc.), tale monitoraggio è configurato per generare avvisi per il personale?	<ul style="list-style-type: none"> Esaminare le impostazioni di configurazione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.1 Viene mantenuto un inventario dei punti di accesso wireless autorizzati e viene documentata una giustificazione aziendale per tutti i punti di accesso wireless autorizzati?	<ul style="list-style-type: none"> Esaminare i record di inventario 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
11.1.2	(a) Il piano di risposta agli incidenti definisce e richiede una risposta in caso di rilevamento di punti di accesso wireless non autorizzati?	<ul style="list-style-type: none"> Esaminare il piano di risposta agli incidenti (vedere il Requisito 12.10) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Viene intrapresa un'azione quando si rilevano punti di accesso wireless non autorizzati?	<ul style="list-style-type: none"> Consultare il personale responsabile Ispezionare le scansioni wireless recenti e le relative risposte 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2	<p>Sono state eseguite scansioni interne ed esterne della rete almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, l'installazione di nuovi componenti di sistema, la modifica della topologia della rete, la modifica delle regole del firewall o l'aggiornamento di un prodotto), come segue?</p> <p>Nota: è possibile unire più rapporti delle scansioni per il processo di scansione trimestrale per accertarsi che sia stata eseguita la scansione di tutti i sistemi e siano state risolte tutte le vulnerabilità applicabili. Potrebbe essere necessaria una documentazione ulteriore per verificare che le vulnerabilità non corrette siano in fase di correzione.</p> <p>Per la conformità iniziale a PCI DSS, non è necessario che vengano completati quattro scansioni trimestrali positive se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) le vulnerabilità rilevate nei risultati della scansione sono state corrette nel modo dimostrato da una nuova scansione. Per gli anni successivi alla revisione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.</p>					

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
11.2.1	(a) Vengono eseguite scansioni interne di vulnerabilità trimestrali?	<ul style="list-style-type: none"> Analizzare i rapporti delle scansioni 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Il processo di scansioni interne trimestrali risolve tutte le vulnerabilità "Elevate" e comprende nuove scansioni fino alla risoluzione di tutte le vulnerabilità "Elevate" (come definito nel Requisito 6.1 PCI DSS)?	<ul style="list-style-type: none"> Analizzare i rapporti delle scansioni 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Le scansioni interne trimestrali vengono eseguite da una risorsa interna o da una terza parte qualificata e, se applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> Consultare il personale 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2	(a) Vengono eseguite scansioni esterne di vulnerabilità trimestrali? <i>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di prodotti di scansione approvato (ASV) e autorizzato dall'Ente responsabile degli standard di protezione PCI (PCI SSC). Fare riferimento alla Guida del programma ASV pubblicata sul sito Web PCI SSC per le responsabilità dei clienti relative alle scansioni, la preparazione delle scansioni, ecc.</i>	<ul style="list-style-type: none"> Analizzare i risultati dai quattro trimestri più recenti di scansioni delle vulnerabilità esterne 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I risultati delle scansioni esterne trimestrali soddisfano i requisiti della Guida del programma per i fornitori di scansioni approvati (ad esempio nessuna vulnerabilità classificata superiore a 4.0 dal CVSS e nessun errore automatico)?	<ul style="list-style-type: none"> Analizzare i risultati di ogni scansione trimestrale esterna e ripetere la scansione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Le scansioni esterne di vulnerabilità trimestrali vengono eseguite dal fornitore di prodotti di scansione approvato (ASV) PCI SSC?	<ul style="list-style-type: none"> Analizzare i risultati di ogni scansione trimestrale esterna e ripetere la scansione 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Si	Si con CCW	No	N/A
11.2.3	(a) Le scansioni interne ed esterne vengono eseguite, e ripetute se necessario, dopo ogni modifica significativa? <i>Nota: le scansioni devono essere eseguite da personale qualificato.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Il processo di scansione comprende nuove scansioni fino a quando: <ul style="list-style-type: none"> Per le scansioni esterne, non esistano vulnerabilità a cui sia assegnato un punteggio superiore a 4.0 da parte del CVSS. Per le scansioni interne, sia stato conseguito un risultato positivo oppure siano state risolte tutte le vulnerabilità "Elevate" in base alla definizione contenuta nel Requisito 6.1 PCI DSS? 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Le scansioni vengono eseguite da una risorsa interna o da una terza parte qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.4	Se si utilizza la segmentazione per isolare l'ambiente dei dati dei titolari di carta da altre reti:				
	(a) Sono state definite procedure dei test di penetrazione per testare tutti i metodi di segmentazione e confermare che sono funzionali ed efficaci, e isolare tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
	(b) I test di penetrazione volti a verificare i controlli di segmentazione rispondono ai seguenti criteri? <ul style="list-style-type: none"> • Vengono eseguiti almeno una volta all'anno e dopo eventuali modifiche ai controlli/metodi di segmentazione. • Coprono tutti i controlli/metodi di segmentazione in uso. • Verificano che i metodi di segmentazione siano funzionali ed efficaci e isolino tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE. 	<ul style="list-style-type: none"> ▪ Esaminare i risultati dai test di penetrazione più recenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) I test sono eseguiti da una risorsa interna o da una terza parte esterna qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> ▪ Consultare il personale responsabile 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5	(a) È stato implementato un meccanismo di rilevamento delle modifiche (ad esempio, strumenti di monitoraggio dell'integrità file) per rilevare modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) a file di sistema, di configurazione o di contenuti critici? <p><i>Tra gli esempi di file che devono essere monitorati:</i></p> <ul style="list-style-type: none"> • Eseguibili di sistema • eseguibili di applicazioni • File di configurazione e parametri • File memorizzati centralmente, di cronologia o archiviazione, di registro e audit • File critici ulteriori determinati dall'entità (ad esempio, tramite la valutazione dei rischi o altri mezzi) 	<ul style="list-style-type: none"> ▪ Osservare le impostazioni di sistema e i file monitorati ▪ Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
	<p>(b) Il meccanismo di rilevamento delle modifiche è stato configurato per segnalare al personale le modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) ai file di sistema, di configurazione o di contenuti critici? Questi strumenti eseguono confronti di file critici almeno una volta alla settimana?</p> <p>Nota: ai fini del rilevamento delle modifiche, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. I meccanismi di rilevamento delle modifiche come i prodotti per il monitoraggio dell'integrità dei file sono generalmente preconfigurati con file critici per il sistema operativo in uso. Altri file critici, ad esempio quelli per applicazioni personalizzate, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).</p>	<ul style="list-style-type: none"> Osservare le impostazioni di sistema e i file monitorati Analizzare i risultati delle attività di monitoraggio 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5.1	È stato adottato un processo per rispondere a eventuali avvisi generati dalla soluzione di rilevamento delle modifiche?	<ul style="list-style-type: none"> Esaminare le impostazioni di configurazione del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Gestire una politica di sicurezza delle informazioni

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

Nota: ai fini del Requisito 12, per “personale” si intende un dipendente a tempo pieno o part-time, un dipendente con contratto a tempo determinato, un collaboratore o consulente che svolge le sue prestazioni in sede o che abbia in altro modo accesso all’ambiente dei dati dei titolari di carta della società.

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	Autenticazione per l'uso della tecnologia?	▪ Analizzare le politiche di utilizzo ▪ Consultare il personale responsabile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	Usi accettabili delle tecnologie?	▪ Analizzare le politiche di utilizzo ▪ Consultare il personale responsabile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	Posizioni di rete accettabili per le tecnologie?	▪ Analizzare le politiche di utilizzo ▪ Consultare il personale responsabile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
12.3.8	Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività?	<ul style="list-style-type: none"> Analizzare le politiche di utilizzo Consultare il personale responsabile 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.9	Attivazione di tecnologie di accesso remoto per fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso?	<ul style="list-style-type: none"> Analizzare le politiche di utilizzo Consultare il personale responsabile 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure di sicurezza delle informazioni Consultare un campione di personale responsabile 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure di sicurezza delle informazioni 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Analizzare il programma di consapevolezza della sicurezza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	Vengono mantenute e implementate politiche e procedure per gestire i provider di servizi con cui vengono condivisi i dati dei titolari di carta o che potrebbero incidere sulla sicurezza dei dati dei titolari di carta, come segue:					
12.8.1	È stato conservato un elenco di provider di servizi, inclusa una descrizione dei servizi forniti?	<ul style="list-style-type: none"> Analizzare le politiche e le procedure Osservare i processi Analizzare un elenco dei provider di servizi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Si	Si con CCW	No	N/A
12.8.2	<p>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?</p> <p>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.</p>	<ul style="list-style-type: none"> ▪ Osservare i contratti scritti ▪ Analizzare le politiche e le procedure 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	Esiste un processo definito per incaricare i provider di servizi, che includa tutte le attività di "due diligence" appropriate prima dell'incarico?	<ul style="list-style-type: none"> ▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	È stato conservato un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi con cadenza almeno annuale?	<ul style="list-style-type: none"> ▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	Vengono conservate le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità?	<ul style="list-style-type: none"> ▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Si	Si con CCW	No	N/A
12.10.1 (a) È stato creato un piano di risposta da implementare in caso di violazione del sistema?	<ul style="list-style-type: none"> ▪ Analizzare il piano di risposta agli incidenti ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Il piano include almeno i seguenti elementi?					
<ul style="list-style-type: none"> • Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Procedure specifiche di risposta agli incidenti 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Procedure di ripristino e continuità delle attività aziendali 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Processi di backup dei dati 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Analisi dei requisiti legali per la segnalazione di violazioni 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Copertura e risposte per tutti i componenti di sistema critici 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento 	<ul style="list-style-type: none"> ▪ Analizzare le procedure per il piano di risposta agli incidenti 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Appendice A - Requisiti PCI DSS aggiuntivi

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

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

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

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
			Sì	Sì con CCW	No	N/A
A2.1	<p>Per i terminali POS POI (e i punti di terminazione SSL/TLS a cui si connettono) che utilizzano SSL e/o TLS iniziale:</p> <ul style="list-style-type: none"> 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? 	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)			
		Sì	Sì con CCW	No	N/A
<p>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:</p> <ul style="list-style-type: none"> ▪ 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? 	<ul style="list-style-type: none"> ▪ Analizzare il piano documentato di migrazione e di riduzione dei rischi 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Appendice A3 - Convalida aggiuntiva delle entità designate (DESV)

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

Appendice B - Foglio di lavoro - Controlli compensativi

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito per il quale è stata selezionata la risposta “Sì con CCW”.

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

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

Numero e definizione del requisito:

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

Sezione 3 - Dettagli su convalida e attestato

Parte 3. Convalida PCI DSS

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

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

<input type="checkbox"/>	<p>Conforme: Tutte le sezioni del questionario PCI DSS SAQ sono state completate e a tutte le domande è stato risposto in modo affermativo, determinando una valutazione di CONFORMITÀ globale; pertanto (<i>Ragione sociale esercente</i>) ha dimostrato la massima conformità agli standard PCI DSS.</p>						
<input type="checkbox"/>	<p>Non conforme: non tutte le sezioni del questionario PCI DSS SAQ sono state completate o non a tutte le domande è stata fornita una risposta affermativa, determinando una valutazione di NON CONFORME globale; pertanto (<i>Ragione sociale esercente</i>) non ha dimostrato la massima conformità agli standard PCI DSS.</p> <p>Data di destinazione per conformità:</p> <p>è possibile che a un'entità che invia questo modulo con lo stato "Non conforme" venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. <i>Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4.</i></p>						
<input type="checkbox"/>	<p>Conforme ma con eccezione legale: uno o più requisiti sono stati contrassegnati con "No" a causa di una restrizione legale che impedisce di rispondere al requisito. Questa opzione richiede un'ulteriore revisione da parte dell'acquirente o del marchio di pagamento.</p> <p><i>Se selezionata, completare quanto segue:</i></p> <table border="1" data-bbox="289 1134 1409 1304"> <thead> <tr> <th>Requisito interessato</th> <th>Dettagli su come il vincolo legale impedisce la conformità ai requisiti</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti				
Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti						

Parte 3a. Riconoscimento dello stato

I firmatari confermano:

(*Selezionare tutte le risposte pertinenti*)

<input type="checkbox"/>	Il questionario di autovalutazione C PCI DSS, versione (<i>versione di SAQ</i>), è stato completato in base alle istruzioni qui fornite.
<input type="checkbox"/>	Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione sotto tutti gli aspetti.
<input type="checkbox"/>	Ho verificato con il fornitore dell'applicazione di pagamento che il mio sistema di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
<input type="checkbox"/>	Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard in ogni momento, in base a quanto applicabile al mio ambiente.
<input type="checkbox"/>	Se il mio ambiente cambia, accetto di dover rivalutare l'ambiente e implementare eventuali requisiti PCI DSS in base alle necessità.

Parte 3a. Riconoscimento dello stato (continua)

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

Parte 3b. Attestato esercente

Firma del funzionario esecutivo dell'esercente ↑	Data:
Nome del funzionario esecutivo dell'esercente:	Mansione:

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

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

Firma del funzionario espressamente autorizzato dell'azienda QSA ↑	Data:
Nome del funzionario espressamente autorizzato:	Azienda QSA:

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

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

¹ Dati codificati nella striscia magnetica o dati equivalenti su un chip utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare i dati della traccia completa dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il PAN, la data di scadenza e il nome del titolare della carta.

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

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

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

Selezionare la risposta appropriata per "Conforme ai requisiti PCI DSS" per ogni requisito. In caso di risposta negativa a uno dei requisiti, è necessario fornire la data in cui si prevede che la Società sarà conforme al requisito e una breve descrizione delle azioni che verranno intraprese per soddisfare il requisito.

Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4.

Requisito* PCI DSS	Descrizione del requisito	Conforme ai requisiti PCI DSS (Selezionarne uno)		Data della soluzione e azioni (Se è stata selezionata l'opzione "NO" per un qualsiasi requisito)
		SÌ	NO	
1	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati dei titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Sviluppare e gestire sistemi e applicazioni protette	<input type="checkbox"/>	<input type="checkbox"/>	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	<input type="checkbox"/>	<input type="checkbox"/>	
8	Individuare e autenticare l'accesso ai componenti di sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
10	Registrazione e monitoraggio di tutti gli accessi a risorse di rete e dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eseguire regolarmente test dei sistemi e processi di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	<input type="checkbox"/>	<input type="checkbox"/>	
Appendice A2	Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale	<input type="checkbox"/>	<input type="checkbox"/>	

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

