



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

**Riepilogo delle modifiche PCI DSS
dalla versione 1.2.1 alla 2.0**

Ottobre 2010

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Aspetti generali	Aspetti generali	<p>In tutto il documento</p> <p>Eliminati i riferimenti specifici al Glossario, in quanto, in linea generale, non sono forniti per altri termini del glossario.</p>	Chiarimento
Aspetti generali	Aspetti generali	<p>Attestati di conformità</p> <ul style="list-style-type: none"> ▪ Attestati di conformità eliminati dalle appendici e creazione di documenti a parte. ▪ Riferimenti e titoli di appendici aggiornati di conseguenza in tutto il documento. 	Chiarimento
Aspetti generali	Aspetti generali	<p>Introduzione e panoramica di PCI Data Security Standard</p> <ul style="list-style-type: none"> ▪ Aggiunte informazioni sul ruolo svolto da PCI DSS per la protezione dei dati dei titolari di carta. ▪ Aggiornata la grafica 'Panoramica di alto livello' per riflettere i titoli dei requisiti. ▪ Chiarito che PCI DSS è uno strumento di valutazione da usare nel corso delle valutazioni di conformità. ▪ Aggiunte informazioni sulle risorse disponibili sul sito Web PCI SCC. 	Ulteriori istruzioni
Aspetti generali	Aspetti generali	<p>Informazioni sull'applicabilità degli standard PCI DSS</p> <ul style="list-style-type: none"> ▪ Aggiunto termine <i>"dati di account"</i> in linea con il modulo PTS SRED (Secure Exchange and Reading of Data). ▪ Forniti ulteriori dettagli su <i>"dati del titolare di carta"</i> e <i>"dati sensibili di autenticazione"</i>. ▪ Chiarito che il PAN (primary account number) è il fattore di definizione per l'applicabilità degli standard PCI DSS. ▪ Eliminata nota a piè di pagina che rimanda ad altra legislazione e sostituita con un testo di paragrafo aggiornato. ▪ Aggiornati testo paragrafo e tabella di applicabilità per chiarire che gli elementi di dati devono essere resi illeggibili in conformità al Requisito 3.4 PCI DSS. 	Chiarimento
N/A	Aspetti generali	<p>Relazione tra PCI DSS e PA-DSS</p> <ul style="list-style-type: none"> ▪ Aggiunta nuova sezione per riflettere i contenuti in PA-DSS. ▪ Chiarito che l'uso della sola applicazione conforme agli standard PA-DSS non rende l'entità conforme a tali standard. 	Ulteriori istruzioni

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Aspetti generali	Aspetti generali	<p>Ambito della valutazione per la conformità ai requisiti PCI DSS</p> <ul style="list-style-type: none"> ▪ Aggiunto “componenti di virtualizzazione” alla definizione di “componenti di sistema”. ▪ Chiarito che l'ambiente dei titolari di carta di credito è composto da “persone, processi e tecnologia che memorizzano, elaborano o trasmettono dati dei titolari di carta o dati sensibili di autenticazione”. 	Ulteriori istruzioni
Aspetti generali	Aspetti generali	<p>Ambito della valutazione per la conformità ai requisiti PCI DSS</p> <p>Aggiunto paragrafo dettagliato per chiarire che il primo passo di una revisione PCI DSS consiste nello stabilire con precisione l'ambito della valutazione, individuando tutte le posizioni ed i flussi di dati dei titolari di carte e garantendo l'inserimento di tutte queste posizioni nella valutazione.</p>	Ulteriori istruzioni
Aspetti generali	Aspetti generali	<p>Segmentazione di rete</p> <ul style="list-style-type: none"> ▪ Aggiunti chiarimenti compreso che la segmentazione si può ottenere attraverso mezzi fisici o logici. ▪ Correzioni di lieve entità per chiarire il significato. 	Chiarimento
Aspetti generali	Aspetti generali	<p>Wireless</p> <p>Chiarito il punto centrale sulla presenza di una WLAN piuttosto che di una LAN.</p>	Chiarimento
Aspetti generali	Aspetti generali	<p>Terze parti/Outsourcing</p> <p>Cambiamenti di lieve entità alla terminologia per congruenza.</p>	Chiarimento
Aspetti generali	Aspetti generali	<p>Campionamento delle strutture aziendali e dei componenti di sistema</p> <ul style="list-style-type: none"> ▪ Chiarito che il campionamento viene realizzato in modo indipendente dal valutatore e che il campionamento deve essere eseguito prima per le strutture aziendali e quindi per i componenti di sistema all'interno della struttura selezionata. ▪ Chiarito che il campionamento non riduce l'ambito dell'ambiente dei dati dei titolari di carta o l'applicabilità degli standard PCI DSS e che non è consentito il campionamento dei singoli requisiti PCI DSS. ▪ Chiariti i criteri specifici che i valutatori sono tenuti a documentare quando fanno ricorso al campionamento. Aggiunto il criterio che i valutatori devono convalidare di nuovo il motivo del campionamento per ogni valutazione. 	Ulteriori istruzioni

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Aspetti generali	Aspetti generali	<p>Istruzioni e contenuto per il rapporto sulla conformità</p> <ul style="list-style-type: none"> ▪ Aggiunti i criteri per i valutatori per descrivere in che modo la precisione dell'ambito PCI DSS sia stata convalidata per la valutazione, nella parte 2. ▪ Aggiornati i dettagli di rendicontazione per il motivo alla base del campionamento e la convalida della dimensione del campione nella parte 2, in linea con i contenuti chiariti nella sezione Campionamento. ▪ Nella parte 3, chiarito che l'elenco delle persone intervistate deve includere le rispettive organizzazioni di appartenenza e gli argomenti trattati. ▪ Spostato "Tempi di valutazione" dalla parte 2 alla parte 4, e aggiunto che nel tempo deve indicare la durata e specificare il periodo di tempo nel corso del quale è avvenuta la valutazione. ▪ Cambiato "Procedure di scansione della sicurezza PCI DSS" in "Guida del programma per i fornitori di scansioni approvati" nella parte 5. ▪ Aggiunta spiegazione per risposte N/A nella parte 6. ▪ Modifiche di lieve entità per congruenza. 	Ulteriori istruzioni
Aspetti generali	Aspetti generali	<p>Conformità agli standard PCI DSS – Operazioni</p> <p>Aggiornato riferimento agli Attestati di conformità sul sito Web PCI SSC.</p>	Chiarimento
Aspetti generali	Aspetti generali	<p>Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate</p> <p>Aggiunto chiarimento che le risposte N/A devono essere riportate nella colonna "Presente".</p>	Chiarimento
1	1	<p>Paragrafo introduttivo</p> <ul style="list-style-type: none"> ▪ Modifiche di lieve entità per congruenza. ▪ Aggiunta spiegazione che gli altri componenti di sistema che forniscono funzionalità firewall devono essere trattati in conformità al Requisito 1. 	Ulteriori istruzioni
1.1.3	1.1.3.a, 1.1.3.b	<p>Procedure di test</p> <p>Separata la procedura di test 1.1.3. in due singole procedure 1.3.a - 1.3.b.</p>	Chiarimento
1.1.5	1.1.5	<p>Requisito</p> <p>Aggiunti esempi di servizi, protocolli o porte non sicuri.</p>	Ulteriori istruzioni

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
1.2	1.2	Requisito Aggiornato requisito per allinearlo alla procedura di test.	Chiarimento
1.3	1.3	Procedura di test Riorganizzato per chiarire lo scopo della procedura.	Chiarimento
1.3.1	1.3.1	Requisito e procedura di test Chiarito lo scopo del requisito per la zona DMZ per limitare il traffico in entrata ai componenti di sistema che forniscono servizi, protocolli e porte autorizzati.	Chiarimento
1.3.3	1.3.3	Requisito e procedura di test Chiarito che non si devono consentire le connessioni dirette tra Internet e le reti interne.	Chiarimento
1.3.5	1.3.5	Requisito e procedura di test Chiarito lo scopo che è consentito solo il traffico in uscita autorizzato.	Chiarimento
1.3.6	1.3.6	Procedura di test Concessa una maggiore flessibilità nella procedura di test eliminando la specifica dell'uso di scanner di porte.	Chiarimento
1.3.7	1.3.7	Requisito e procedura di test Chiarito che il requisito si applica a qualsiasi tipo di memorizzazione di dati dei titolari di carta, piuttosto che ai soli database.	Chiarimento
1.3.8	1.3.8.a – 1.3.8.b	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Chiarito lo scopo di impedire la divulgazione di indirizzi IP privati a Internet e di garantire che tale eventuale divulgazione ad entità esterne è autorizzata. ▪ Eliminati riferimenti specifici all'IP-masquerading ed all'uso di tecnologie NAT (Network Address Translation) ed aggiunti esempi di metodi volti ad impedire la divulgazione di indirizzi IP privati. ▪ Separata la procedura di test in due sotto-procedure. 	Ulteriori istruzioni
1.4.b	1.4.b	Procedura di test Chiarito che il software firewall personale non deve essere modificabile da utenti di computer di proprietà dei dipendenti per allineare la procedura di test al requisito.	Chiarimento
2.1	2.1	Requisito Modifiche di lieve entità per chiarezza.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
2.1.1	2.1.1.a – 2.1.1.e	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Eliminati i contenuti che si sovrapponevano al Requisito 4.1.1, per chiarire che questo requisito ha lo scopo di garantire che le impostazioni predefinite del fornitore sono modificate. ▪ Separata la procedura di test 2.1.1 in singole procedure da 2.1.1.a a 2.1.1.e. ▪ Eliminato il riferimento a WPA poiché non viene più considerata crittografia avanzata da sola. 	Chiarimento
2.2	2.2	Requisito e procedure di test Sposati gli esempi di standard di System Hardening dalla procedura di test al requisito ed aggiunta ISO come fonte di standard di hardening.	Chiarimento
6.2.b	6.2.b	Procedura di test Spostati contenuti dalla precedente Procedura di test 6.2.b a 2.2.b per garantire che gli standard di configurazione del sistema siano aggiornati con le vulnerabilità identificate dal Requisito 6.2.	Chiarimento
2.2.b	2.2.d	Procedura di test Rinumerata la procedura di test da 2.2.b a 2.2.d	Chiarimento
2.2.1	2.2.1	Requisito Aggiornato il requisito per chiarire lo scopo di “una funzione primaria per server” e l'uso della virtualizzazione.	Ulteriori istruzioni
N/A	2.2.1.b	Procedure di test <ul style="list-style-type: none"> ▪ Nuova procedura di test facoltativa per le tecnologie di virtualizzazione. ▪ Rinumerata la procedura di test da 2.2.1 a 2.2.1.a. 	Ulteriori istruzioni
2.2.2	2.2.2, 2.2.2.a – 2.2.2.b	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che solo i servizi, protocolli, daemon ecc. sicuri e necessari devono essere attivati e le funzioni di sicurezza implementate per ogni tale servizio ecc. non sicuro, con esempi. ▪ Separata la procedura di test 2.2.2 in singole procedure 2.2.2.a e 2.2.2.b. 	Chiarimento
2.2.4	2.2.4.a - 2.2.4.c	Procedure di test Separata la procedura di test 2.2.4 in singole procedure da 2.2.4.a a 2.2.4.c.	Chiarimento
2.3	2.3, 2.3.a – 2.3.c	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che è necessaria la crittografia avanzata. ▪ Separata la procedura di test 2.3 in singole procedure da 2.3.a a 2.3.c. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
3	3	Paragrafo introduttivo Chiarito che <i>“i PAN senza protezione non devono essere inviati utilizzando tecnologie di messaggistica degli utenti finali come e-mail e messaggistica istantanea.”</i>	Chiarimento
3.1	3.1	Requisito e procedure di test Attribuito a questo requisito un carattere più generale e spostate le procedure di test precedentemente in 3.1 in un nuovo Requisito e procedura di test 3.1.1 (vedere di seguito).	Chiarimento
N/A	3.1.1, 3.1.1.a – 3.1.1.e	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Separata la procedura di test 3.1 in singole procedure da 3.1.1.a a 3.1.1.d. ▪ Aggiunti dettagli al requisito per allinearli alle procedure di test. ▪ Nuova Procedura di test 3.1.1.e per chiarire che il valutatore è tenuto a verificare che i dati memorizzati non superino i requisiti di conservazione indicati nella politica. 	Chiarimento
3.2	3.2	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Aggiunta nota al requisito per chiarire che per emittenti e società che supportano servizi di elaborazione di emissione è ammissibile memorizzare dati sensibili di autenticazione in presenza di una giustificazione aziendale e di una memorizzazione sicura dei dati. ▪ Nuova procedura di test 3.2.a aggiunta per emittenti e società che supportano servizi di emissione per verificare l'esistenza della giustificazione aziendale se sono memorizzati dati sensibili di autenticazione. ▪ Rinumerata procedura di test da 3.2 a 3.2.b, inserendo prima <i>“Per tutte le altre entità ”</i>. 	Chiarimento
3.2.1	3.2.1	Requisito e procedura di test Sostituito <i>“contenuto in un chip”</i> con <i>“dati equivalenti su un chip”</i> per congruenza.	Chiarimento
3.2.1 – 3.2.3	3.2.1 – 3.2.3	Procedure di test Chiarite le procedure di test per <i>“esaminare i file di dati, incluso, senza limitazione, quanto segue”</i> .	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
3.4	3.4	Requisito <ul style="list-style-type: none"> ▪ Chiarito che il requisito è valido solo per il PAN. ▪ Eliminata nota sull'informazione minima sull'account poiché ciò è stato chiarito nel requisito e nella tabella di applicabilità PCI DSS. ▪ Chiariti i requisiti in caso di utilizzo di hashing o troncatura per rendere il PAN illeggibile. ▪ Aggiunta nota per identificare il rischio di PAN in versione hash o troncata nello stesso ambiente, e che ulteriori controlli di sicurezza sono necessari per garantire che non sia possibile ricostruire i dati del PAN originale. ▪ Eliminata nota sull'uso dei controlli compensativi (poiché tali controlli possono essere applicabili a gran parte dei requisiti PCI DSS). 	Chiarimento
3.4.d	3.4.d	Procedura di test Chiarito che il PAN deve essere <i>“reso illeggibile o rimosso”</i> , piuttosto che <i>“modificato o rimosso”</i> , in quanto <i>“rimuovere”</i> rende superfluo <i>“modificare”</i> .	Chiarimento
3.4.1.c	3.4.1.c	Procedura di test Chiarita nota per verificare che se non si utilizza la cifratura su disco per cifrare i supporti rimovibili, sarà necessario utilizzare un altro metodo.	Chiarimento
3.5	3.5	Requisito <ul style="list-style-type: none"> ▪ Chiarito che ogni chiave usata per rendere sicuri i dati dei titolari di carta deve essere protetta da divulgazione e uso improprio. ▪ Aggiunta nota per chiarire come questo requisito si applica alle KEK (key-encrypting key), se utilizzate. 	Chiarimento
3.5.1	3.5.1	Procedura di test Aggiornata procedura di test per allinearla al requisito.	Chiarimento
3.5.2	3.5.2, 3.5.2.a – 3.5.2.b	Requisito e procedure di test Aggiunta procedura di test per allinearla al requisito.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
3.6	3.6	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Spostata nota dalla procedura di test al requisito. ▪ Chiarito nella procedura di test 3.6.b che i provider di servizi devono fornire ai clienti istruzioni per la gestione delle chiavi coprendo trasmissione, memorizzazione e aggiornamento delle chiavi dei clienti (non solo la memorizzazione), in conformità ai Sottorequisiti da 3.6.1 a 3.6.8. ▪ Cancellata nota sulla trasmissione sicura di tali chiavi in quanto tale argomento è coperto nei sottorequisiti. 	Chiarimento
3.6.4	3.6.4	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Chiarito che le modifiche delle chiavi sono necessarie una volta terminato il loro periodo di validità definito, piuttosto che <i>“almeno annualmente”</i>. ▪ Aggiunte linee guida per le migliori pratiche del settore. 	Chiarimento
3.6.5	3.6.5	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Modificato contenuto per chiarire che le chiavi devono essere ritirate o sostituite quando la loro integrità è stata indebolita e forniti esempi. ▪ Aggiunta nota che in caso di conservazione delle chiavi ritirate o sostituite, devono essere archiviate e conservate in modo sicuro solo a fini di decifratura o verifica. ▪ Aggiunta procedura di test per verificare che, in caso di conservazione delle chiavi ritirate o sostituite, esse non vengano usate per operazioni di cifratura. 	Chiarimento
3.6.6	3.6.6	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Chiarito che <i>“split knowledge e controllo duale”</i> si applicano solo alle operazioni di gestione delle chiavi utilizzate per la crittografia con testo in chiaro manuali. ▪ Aggiunta nota per fornire esempi di operazioni di gestione delle chiavi. 	Chiarimento
3.6.8	3.6.8	Requisito e procedura di test Chiarito che i custodi delle chiavi devono <i>“riconoscere in modo formale”</i> le loro responsabilità come custodi delle chiavi piuttosto che <i>“firmare un modulo”</i> .	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
4.1	4.1, 4.1.a – 4.1.e	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Inclusa SSH come esempio di protocollo di sicurezza, eliminati gli esempi dalla procedura di test. ▪ Separata la procedura di test 4.1 in singole procedure da 4.1.a a 4.1.e. ▪ Chiarito nella procedura di test 4.1.b che chiavi e/o certificati affidabili sono necessari per tutti i tipo di trasmissioni, non solo SSL/TLS. ▪ Chiarito nella procedura 4.1.c che il protocollo deve essere implementato per usare configurazioni sicure. 	Chiarimento
4.1.1	4.1.1	Requisito Aggiornata nota relativa all'uso di WEP a partire dal 30 giugno 2010.	Chiarimento
4.2	4.2	Requisito e procedure di test Modificato contenuto per chiarire che PAN non protetti (piuttosto che non criptati) non devono mai essere inviati dalle tecnologie di messaggistica degli utenti finali.	Chiarimento
5.2	5.2	Requisito e procedure di test Chiarito che i meccanismi anti-virus devono generare log di audit, piuttosto che essere solo “capaci di generare” tali log.	Chiarimento
6.1	6.1	Requisiti Chiarito lo scopo di proteggere i componenti di sistema ed il software dalle vulnerabilità note.	Chiarimento
6.2	6.2	Requisito e procedure di test Inserito che oltre ad identificare le vulnerabilità, i processi devono comprendere la classificazione delle vulnerabilità in base al rischio. Fornite istruzioni sulle modalità di assegnazione della classificazione dei rischi. <i>Nota: La classificazione delle vulnerabilità come riportata al punto 6.2.a è considerata una delle migliori pratiche fino al 30 giugno 2012; successivamente a tale data, diventerà un requisito.</i>	Requisito in evoluzione
6.3	6.3, 6.3.a – 6.3.d	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Aggiunti tipi di applicazioni software per le quali sarebbero valide le pratiche di sviluppo sicuro. ▪ Separata la procedura di test 6.3.a in singole procedure da 6.3.a a 6.3.d. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
6.3.1	N/A	Requisiti e procedure di test Eliminati requisiti e procedure di test in quanto i test di vulnerabilità descritti in precedenza al punto 6.3.1 sono ora inseriti nei punti da 6.5.1 a 6.5.9.	Chiarimento
6.3.2 – 6.3.5	6.4.1 – 6.4.4	Requisiti e procedure di test Spostati requisiti e procedure di test al punto 6.4, per chiarire lo scopo che i requisiti si applicano ad ambienti di sviluppo e test e non solo ai primi.	Chiarimento
6.3.6 – 6.3.7	6.3.1 – 6.3.2	Requisiti e procedure di test Rinumerati requisiti e procedure di test a causa dell'unione e/o dello spostamento dei requisiti precedenti.	Chiarimento
6.3.7	6.3.2	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Eliminato dalla nota il riferimento circolare. ▪ Consolidate le procedure di test (in precedenza 6.3.7.a e 6.3.7.b) in un'unica procedura 6.3.2.a, per combinare le applicazioni 'interna' e 'web' in una singola procedura. ▪ Eliminato il riferimento specifico alle applicazioni Web ed alla Guida OWASP per consolidare i requisiti di codifica sicura per le applicazioni comprese nell'ambito, incluse le applicazioni non Web. ▪ Rinumerata la procedura di test che in precedenza era 6.3.7.c in 6.3.2.b. 	Chiarimento
6.4	6.4	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che requisito e procedura di test si applicano ai processi ed alle procedure di controllo delle modifiche. ▪ Importati contenuti dalla precedente Procedura di test 6.3. per allinearla alle procedure di test importate in precedenza 6.3.2 – 6.3.5. 	Chiarimento
6.3.4	6.4.3	Procedura di test Eliminato il contenuto <i>“oppure sono modificati prima dell'uso”</i> per chiarire lo scopo.	Chiarimento
6.4, 6.4.a – 6.4.b	6.4.5, 6.4.5.a – 6.4.5.b	Requisito e procedure di test Aggiornato requisito in precedenza 6.4 per allinearla alle precedenti procedure di test 6.4.a – 6.4.b, per risolvere patch di sicurezza e modifiche al software.	Chiarimento
6.4.1 – 6.4.4	6.4.5.1 – 6.4.5.4	Requisiti e procedure di test Rinumerato per allinearla ai requisiti ed alle procedure di test importati (in precedenza 6.3.2 – 6.3.5).	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
6.4.1	6.4.5.1	Procedura di test Chiarito che la documentazione dell'impatto è necessaria nella procedura di test, per essere in linea con il requisito esistente.	Chiarimento
6.4.2	6.4.5.2	Requisito e procedura di test Chiarito nel requisito e nella procedura di test che è necessario ricevere l'approvazione delle "parti autorizzate" piuttosto che del "management."	Chiarimento
6.4.3	6.4.5.3, 6.4.5.3.a – 6.4.5.3.b	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Lo scopo chiarito del requisito e della procedura di test in precedenza 6.4.3 è per "Test della funzionalità per verificare che le modifiche non influiscano negativamente sulla sicurezza del sistema". ▪ Il precedente Requisito 6.3.1 incorporato alla nuova Procedura di test 6.4.5.3.b, in relazione al test delle modifiche del codice personalizzate con riferimento a 6.5. 	Chiarimento
6.5	6.5	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarimento che la codifica sicura e la prevenzione delle vulnerabilità si applica a tutti i tipi di applicazioni sviluppate per i clienti incluse nell'ambito, piuttosto che solo alle applicazioni Web. ▪ Eliminata la dipendenza da OWASP ed inseriti altri esempi del settore SANS CWE e CERT. 	Chiarimento
6.5.1 – 6.5.10	6.5.1 – 6.5.9	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Vulnerabilità in precedenza 6.5.1 – 6.5.10 aggiornate e combinate con il precedente Requisito 6.3.1 per riflettere le attuali istruzioni di CWE, CERT e OWASP. ▪ 6.5.7 – 6.5.9 identificati come vulnerabilità specifiche delle applicazioni Web. 	Chiarimento
N/A	6.5.6	Requisito e procedura di test Aggiunto nuovo requisito e procedura di test per risolvere le vulnerabilità a rischio elevato individuate al Requisito 6.2. <i>Nota: La classificazione delle vulnerabilità come riportata al Requisito 6.2.a è considerata una delle migliori pratiche fino al 30 giugno 2012; successivamente a tale data, diventerà un requisito.</i>	Requisito in evoluzione
7.1.3	7.1.3	Requisito e procedure di test Chiarito requisito per l'approvazione documentata delle parti autorizzate, piuttosto che "un modulo firmato dal management."	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
7.2.3	7.2.3	Requisito e procedure di test Nota spostata dalla procedura di test al requisito.	Chiarimento
8	8	Paragrafo introduttivo Aggiunta nota per essere in linea con il Requisito 3.2 PA-DSS, riguardante l'applicabilità di un ID utente univoco e controlli di autenticazione sicuri per <i>“account utenti all'interno di un'applicazione di pagamento dei punti vendita che ha accesso ad un solo numero di carta alla volta al fine di agevolare una singola transazione (come gli account cassiere).”</i>	Chiarimento
8.2	8.2	Requisito Aggiunto chiarimento ed esempi di metodi di autenticazione.	Chiarimento
8.3	8.3	Requisito e procedura di test Chiariti esempi di autenticazione a due fattori per comprendere Radius <i>“con token”</i> e <i>“altre tecnologie che supportano l'autenticazione avanzata .”</i> Aggiunta nota per chiarire lo scopo dell'autenticazione a due fattori.	Chiarimento
8.5	8.5	Requisiti e procedure di test Aggiunto termine <i>“identificazione.”</i>	Chiarimento
8.5.2, 8.5.7, 8.5.8, 8.5.13	8.5.2, 8.5.7, 8.5.8, 8.5.13	Requisiti e procedure di test Aggiunto <i>“autenticazione”</i> per tener conto di una maggiore flessibilità per le società che utilizzano altri meccanismi di autenticazione diversi dalle password.	Chiarimento
8.5.3	8.5.3	Requisito e procedure di test Incluso <i>“ripristino delle password”</i> che rende necessari valore univoco e modifica immediata dopo il primo uso.	Chiarimento
8.5.6	8.5.6, 8.5.6.a – 8.5.6.b	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito <i>“accesso”</i> da parte dei fornitori. Aggiornato requisito per allinearli alla procedura di test. ▪ Separata la procedura di test 8.5.6 in due singole procedure 8.5.6.a - 8.5.6.b. 	Chiarimento
8.5.9 – 8.5.13	8.5.9 – 8.5.13	Procedure di test <ul style="list-style-type: none"> ▪ Chiarire i requisiti di gestione delle password per <i>“utenti non consumatori”</i> dal punto di vista del provider di servizi. ▪ Separata singola procedura di test per differenziare la procedura per provider di servizi, per ogni requisito. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
8.5.16, 8.5.16.a	8.5.16, 8.5.16.a – 8.5.16.d	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che la limitazione di query ed accesso diretto al database è valida per l'accesso utenti. ▪ Separata la procedura di test 8.5.16.a in singole procedure da 8.5.16.a a 8.5.16.d. 	Chiarimento
9	9	Paragrafo introduttivo <ul style="list-style-type: none"> ▪ Aggiunti termini e definizioni per <i>“personale in sede”, “visitatore” e “supporti”,</i> da usare in tutto il requisito. ▪ Il nuovo termine <i>“personale in sede”</i> sostituisce il vecchio termine <i>“dipendente”</i> con una nuova definizione per chiarire a cosa ci si vuole riferire. 	Chiarimento
9.1.1	9.1.1.a – 9.1.1.c	Procedure di test <ul style="list-style-type: none"> ▪ Separata la precedente procedura di test 9.1.1 in singole procedure di test da 9.1.1.a a 9.1.1.c. ▪ Modificato in <i>“videocamere e/o meccanismi per il controllo dell'accesso”</i> nelle procedure di test, in quanto le videocamere sono meccanismi di monitoraggio dell'accesso che si possono utilizzare con meccanismi per il controllo dell'accesso. 	Chiarimento
9.1.2	9.1.2	Requisito e procedura di test Sostituito <i>“dipendente”</i> con <i>“personale in sede”</i> . Aggiunto esempio di aree fisicamente accessibili.	Chiarimento
9.1.3	9.1.3	Requisito e procedura di test Aggiunto <i>“hardware di rete e comunicazione e linee di telecomunicazione”</i> all'elenco di elementi per limitare l'accesso fisico. Questi elementi erano in precedenza inclusi nel Requisito 9.6.	Chiarimento
9.2, 9.2.a	9.2, 9.2.a – 9.2.b	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Sostituito <i>“dipendente”</i> con <i>“personale in sede”</i>. ▪ Separata la procedura di test 9.2.a in due singole procedure 9.2.a - 9.2.b. 	Chiarimento
9.2.b	9.2.c	Procedure di test Chiarito per verificare che le tessere magnetiche per i visitatori si distinguono facilmente da quelle utilizzate dal personale in sede.	Chiarimento
9.3	9.3	Procedura di test Chiarito che la procedura di test si applica solo ai controlli dei visitatori per essere in linea con il requisito.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
9.3.1	9.3.1	Procedure di test Chiarita procedura in relazione al tentativo di accedere per assicurare che ai visitatori non sia consentito l'accesso a tali aree senza scorta.	Chiarimento
9.3.2	9.3.2, 9.3.2.a – 9.3.2.b	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Sostituito “<i>dipendente</i>” con “<i>personale in sede</i>”. ▪ Separata la procedura di test 9.3.2 in due singole procedure 9.3.2.a - 9.3.2.b. ▪ Chiarito che la Procedura di test 9.3.2.a serve a verificare che vengano utilizzate le tessere magnetiche di identificazione per i visitatori e che sia possibile distinguere i visitatori dai dipendenti. 	Chiarimento
9.4	9.4	Requisito e procedure di test Sostituito “ <i>dipendente</i> ” con “ <i>personale in sede</i> ”.	Chiarimento
9.5	9.5.a – 9.5.b	Procedure di test <ul style="list-style-type: none"> ▪ Separata la procedura di test 9.5 in due singole procedure 9.5.a - 9.5.b. ▪ Chiarito che la Procedura di test 9.5.a serve a verificare la sicurezza fisica del luogo di conservazione. 	Chiarimento
9.6	9.6	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Sostituito “<i>supporti elettronici e cartacei</i>” con “<i>tutti i supporti</i>” come definito nel paragrafo introduttivo. ▪ Spostato “<i>hardware di rete e comunicazione, linee di telecomunicazione</i>” alla Procedura di test 9.1.3. 	Chiarimento
9.7 - 9.9	9.7 - 9.9	Requisiti e Procedure di test Sostituiti i riferimenti a “ <i>supporti contenenti dati dei titolari di carta</i> ” con “ <i>supporti</i> ” in quanto la definizione è già presente nel paragrafo introduttivo.	Chiarimento
9.7.1	9.7.1	Requisito e procedura di test Chiarito che lo scopo è di essere in grado di determinare la sensibilità dei dati sui supporti.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
10.4	10.4, 10.4.1 – 10.4.3	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che lo scopo è di usare la tecnologia per la sincronizzazione dell'ora per sincronizzare le ore e gli orologi di sistema e per garantire che l'ora sia acquisita, distribuita e memorizzata in modo corretto. ▪ Modificati “sincronizzazione dell'ora” e “NTP” in “tecnologia per la sincronizzazione dell'ora” in tutto il 10.4, e chiarito che “NTP” è un esempio di tecnologia per la sincronizzazione dell'ora. ▪ Separata le precedenti Procedure di test da 10.4.a a 10.4.c in nuovi sottorequisiti e Procedure di test da 10.4.1 a 10.4.3 (vedere di seguito). 	Chiarimento
10.4	10.4.1	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Nuovo sottorequisito dalla precedente Procedura di test 10.4.b, per garantire che i sistemi critici abbiano l'ora esatta e coerente. ▪ Riorganizzata la precedente Procedura di test 10.4.b nelle nuove Procedure di test 10.4.1.a e 10.4.1.b, per coprire le modalità di acquisizione e distribuzione dell'ora. 	Chiarimento
10.4	10.4.2	Requisito e procedure di test Nuovo Sottorequisito e Procedure di test 10.4.2.a e 10.4.2.b per chiarire che i dati dell'ora sono protetti e le modifiche alle impostazioni dell'ora sono autorizzate.	Chiarimento
10.4.c	10.4.3	Requisito e procedura di test Riorganizzato il precedente 10.4.c in un nuovo sottorequisito per garantire che l'ora viene fornita da sorgenti accettate dal settore.	Chiarimento
10.7.b	10.7.b	Procedure di test Chiarito che il test deve confermare che i processi dei registri di audit siano in atto per “recuperare immediatamente” i dati di registro, invece che i dati di registro devono essere “immediatamente disponibili” per l'analisi.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
11.1	11.1	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che il processo deve essere disponibile per <i>“rilevare punti di accesso wireless non autorizzati su base trimestrale”</i>. ▪ Aggiunta flessibilità, precisando che i metodi utilizzati possono comprendere scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless e che, indipendentemente dal metodo usato, devono essere sufficienti per rilevare ed identificare eventuali dispositivi non autorizzati. 	Ulteriori istruzioni
11.1.a – 11.1.c	11.1.a – 11.1.e	Procedure di test <ul style="list-style-type: none"> ▪ Separata la procedura di test 11.1.a in singole procedure 11.1.a e 11.1.c. ▪ Aggiunta nuova Procedura di test 11.1.b per verificare che la metodologia sia adeguata per rilevare punti di accesso wireless non autorizzati. ▪ Rinumerata la precedente Procedura di test 11.1.b in 11.1.d e chiarito che la configurazione per generare avvisi al personale si applica in caso di utilizzo del monitoraggio automatico. ▪ Rinumerata la precedente procedura di test 11.1.c in 11.1.e 	Chiarimento
11.2	11.2, 11.2.1 – 11.2.3	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Separati e rinumerati i requisiti di scansione interna ed esterna in precedenza 11.2 in singoli Sottorequisiti e Procedure di test da 11.2.1 a 11.2.3. ▪ Spostata nota dalla precedente Procedura di test 11.2.b al Requisito 11.2 per chiarire devono essere sottoposti a verifica quattro scansioni interne ed esterne. 	Chiarimento
11.2.a	11.2.1.a – 11.2.1.c	Procedura di test <ul style="list-style-type: none"> ▪ Chiarito che il processo di scansione interna comprende l'esecuzione di ulteriori scansioni finché non vengono ottenuti risultati positivi, oppure non sono risolte tutte le vulnerabilità <i>“Elevate”</i> come indicato nel Requisito 6.2 PCI DSS. ▪ Chiarito che le scansioni interne devono essere eseguite da parti qualificate. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
11.2.b	11.2.2.a – 11.2.2.b	Procedure di test <ul style="list-style-type: none"> ▪ Sostituito “<i>Procedure di scansione della sicurezza PCI</i>” con “<i>Requisiti Guida del programma per fornitori di scansioni approvati (ASV)</i>”. ▪ Chiarito che gli ASV sono approvati da PCI SSC (PCI Security Standards Council). 	Chiarimento
11.2.c	11.2.3.a – 11.2.3.c	Procedure di test Chiariti i requisiti per le scansioni interne ed esterne per includere le ulteriori scansioni fino a quando non sono risolte le vulnerabilità di rischio elevato e per specificare che devono essere eseguite da parti qualificate.	Chiarimento
11.3	11.3	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che le vulnerabilità rilevate sfruttabili devono essere risolte. ▪ Separata la procedura di test 11.3.a in due singole procedure 11.3.a - 11.3.b. 	Chiarimento
11.3.2	11.3.2	Requisito e procedura di test Chiarito che i test di penetrazione per le applicazioni devono essere eseguiti per le vulnerabilità pertinenti e comprendere tutti i tipi di applicazioni compresi nell'ambito.	Chiarimento
11.4	11.4	Requisito e procedure di test Chiarito che IDS/IPS controllano il traffico in corrispondenza del perimetro e presso i punti chiave all'interno dell'ambiente dei dati dei titolari di carta (CDE), piuttosto che tutto il traffico nel CDE.	Chiarimento
11.5	11.5, 11.5.a – 11.5.b	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Sostituito “<i>software</i>” con “<i>strumenti</i>” per chiarire il principio che il software commerciale non costituisce l'unico mezzo per soddisfare i requisiti. ▪ Aggiunta Procedura di test 11.5.b per essere in linea con il requisito esistente per segnalare al personale modifiche non autorizzate e per eseguire confronti di file critici almeno una volta alla settimana. 	Chiarimento
12	12	Titolo requisito Sostituito “ <i>dipendenti e collaboratori</i> ” con “ <i>tutto il personale</i> ”.	Chiarimento
12	12	Paragrafo introduttivo Sostituito “ <i>dipendenti</i> ” con “ <i>personale</i> ” con una definizione leggermente rivista.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
12.1	12.1	Procedure di test Sostituito “ <i>dipendenti</i> ” con “ <i>personale.</i> ”	Chiarimento
12.1.2	12.1.2	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Aggiunti esempi di metodologie per la valutazione dei rischi. ▪ Chiarito che il test deve verificare la documentazione per la valutazione dei rischi. 	Ulteriori istruzioni
12.1.3	12.1.3	Requisito Sostituito “ <i>una volta all'anno</i> ” con “ <i>annualmente</i> ”.	Chiarimento
12.3	12.3	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Eliminato “<i>per dipendenti</i>” per maggiore chiarezza. ▪ Aggiunto “<i>tablet</i>” tra gli esempi di tecnologie. 	Chiarimento
12.3.1	12.3.1	Requisito e procedura di test Sostituito “ <i>management</i> ” con “ <i>parti autorizzate</i> ”.	Chiarimento
12.3.4	12.3.4	Requisito e procedura di test Chiarito per tener conto dell'etichettatura logica.	Chiarimento
12.3.9	12.3.9	Requisito e procedura di test Aggiunto “ <i>partner commerciali</i> ” al requisito insieme a “ <i>fornitori</i> ”.	Chiarimento
12.3.10	12.3.10, 12.3.10.a – 12.3.10.b	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Concessa flessibilità per limitare i divieti per il personale non autorizzato. ▪ Rinumerata la procedura di test da 12.3.10 a 12.3.10.a. Aggiunta nuova Procedura di test 12.3.10.b per verificare che il personale debitamente autorizzato protegge i dati dei titolari di carta in conformità ai requisiti PCI DSS. 	Chiarimento
12.4	12.4	Requisiti e procedure di test Sostituito “ <i>dipendenti e collaboratori</i> ” con “ <i>personale</i> ”.	Chiarimento
12.6	12.6	Requisito e procedura di test Sostituito “ <i>dipendenti</i> ” con “ <i>personale</i> ”.	Chiarimento
12.6.1	12.6.1	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Sostituito “<i>dipendenti</i>” con “<i>personale</i>”. ▪ Aggiunta nota per fornire istruzioni sui metodi che cambiano in funzione del ruolo svolto dal personale. 	Ulteriori istruzioni

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
12.6.2	12.6.2	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Sostituito “dipendenti” con “personale”. ▪ Sostituito “società” con “entità”. 	Chiarimento
12.7	12.7	Requisito e procedura di test <ul style="list-style-type: none"> ▪ Sostituito “dipendenti” con “personale”. ▪ Spostato esempio dalla procedura di test al requisito. ▪ Chiarita la nota al Requisito 12.7 da applicare al “personale potenziale da assumere per determinate posizioni.” 	Chiarimento
12.8	12.8	Procedura di test Sostituito “entità da valutare” con “entità” per congruenza.	Chiarimento
12.8.4	12.8.4	Requisiti e procedure di test Chiarito requisito per monitorare lo stato di conformità PCI DSS dei provider di servizi almeno una volta all'anno. Sostituito “entità valutata ” con “entità”.	Ulteriori istruzioni
12.9.1	12.9.1, 12.9.1.a – 12.9.1.b	Procedura di test <ul style="list-style-type: none"> ▪ Aggiunta Procedura di test 12.9.1.b per chiarire che il test deve comprendere la verifica che vengono seguite le procedure documentate. ▪ Rinumerata la procedura di test da 12.9.1 a 12.9.1.a. 	Chiarimento
12.9.3	12.9.3	Procedura di test Chiarito che il personale specifico deve essere disponibile 24 ore su 24, 7 giorni alla settimana per rispondere in caso di incidenti per essere in linea con il requisito.	Chiarimento
Appendice D	Attestato di conformità – Esercenti	Attestato di conformità <ul style="list-style-type: none"> ▪ Eliminato dall'Appendice come documento separato. ▪ Riorganizzate le informazioni di contatto per Valutatore ed Esercente. 	Chiarimento
Appendice E	Attestato di conformità – Provider di servizi	Attestati di conformità <ul style="list-style-type: none"> ▪ Eliminato dall'Appendice come documento separato. ▪ Riorganizzate le informazioni di contatto per Valutatore e Fornitore di servizi. ▪ Ulteriori opzioni aggiunte nell'elenco di “Servizi che erano inclusi nell'Ambito della valutazione PCI DSS”, ed aggiunto elenco di servizi non coperti dalla valutazione PCI DSS. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Appendice F	Appendice D	Segmentazione e campionamento di strutture aziendali / componenti di sistema <ul style="list-style-type: none"> ▪ Modificato il nome per chiarire il flusso di processo per segmentazione e campionamento. ▪ Creati titoli di sezione separati per campionamento e segmentazione di rete. ▪ Aggiornato per allinearli alla sezione sul campionamento nell'introduzione. 	Chiarimento

ⁱ Spiegazioni di “Tipo”:

Nuovo tipo	Vecchio tipo	Definizione
Chiarimento	Chiarimento	Maggiori informazioni sullo scopo del requisito. Assicurare che il contenuto sintetico negli standard presenti lo scopo dei requisiti che si desidera.
Ulteriori istruzioni	Spiegazione	Spiegazioni e/o definizioni per fornire una maggiore comprensione o ulteriori informazioni su un determinato argomento.
Requisito in evoluzione	Miglioramento	Modifiche per assicurare che gli standard siano aggiornati alle minacce emergenti ed ai cambiamenti del mercato.