



La conformità allo standard Payment Card Industry Data Security Standard (PCI DSS), che impone i requisiti di sicurezza a commercianti, fornitori di servizi e banche che gestiscono le informazioni relative a carte di pagamento, richiede un insieme di adempimenti differenziati in funzione del volume delle operazioni trattate. Quantunque per la maggioranza delle organizzazioni tali adempimenti facciano riferimento ad un set ridotto di requisiti PCI, l'adozione di un livello di approfondimento maggiore di quello strettamente richiesto dalle attività di self assessment consente di prevedere un insieme di misure di sicurezza più completo e con migliori modalità di implementazione.

## Compliance PCI-DSS: trasformare l'obbligo in un'opportunità

Mauro Cosmi

ICTSecurity, marzo 2008

### Livelli di Compliance e requisiti

Gli adempimenti richiesti a merchant e fornitori di servizi, che costituiscono il prerequisito per la conformità allo standard PCI-DSS già introdotto in un precedente articolo, sono differenziati in funzione del ruolo (merchant/service provider) e del volume delle transazioni trattate. La tabella seguente dettaglia i requisiti per la compliance relativi ai merchant, in funzione della categoria di

Merchant Level	Definizione	Compliance Requirements	Validazione
Level 1	<ul style="list-style-type: none"> <li>Tutti merchant con più di 6 milioni di transazioni Visa/Mastercard all'anno, Includendo il canale e-commerce</li> <li>Tutti 1 merchant che hanno subito un attacco informatico che ha compromesso dati di carte di credito</li> <li>Tutti i merchant ai quali Visa/ Mastercard, a loro discrezione, richiedono &lt;S soddisfare 1 requisiti di Livello 1</li> <li>Tutti i merchant ai quali altri player di circuiti di pagamento richiedono di soddisfare 1 requisiti di Livello 1</li> </ul>	<ul style="list-style-type: none"> <li>PCI-DSS Onsite Assessment annuale</li> </ul>	<ul style="list-style-type: none"> <li>Merchant Internal Auditing (*)</li> <li>Auditor esterno (*)</li> <li>Qualified Security Auditor (*)</li> <li>(*) In alternativa</li> </ul>
		<ul style="list-style-type: none"> <li>Network Scan trimestrale</li> </ul>	« Approved Scanning Vendor
Level 2	<ul style="list-style-type: none"> <li>Tutti merchant con un numero di transazioni Visa/Mastercard all'anno compreso tra 1 milione e 6 milioni, Includendo il canale e-commerce.</li> <li>Tutti 1 merchant ai quali altri player di circuiti di pagamento richiedono di soddisfare 1 requisiti di Livello 2</li> </ul>	<ul style="list-style-type: none"> <li>Self Assessment annuale</li> </ul>	• Merchant
		<ul style="list-style-type: none"> <li>Network Scan trimestrale</li> </ul>	• Approved Scanning Vendor
Level 3	<ul style="list-style-type: none"> <li>Tutti merchant con un numero di transazioni Visa/Mastercard all'anno compreso tra 20 mila e 1 milione. Includendo il canale e-commerce.</li> <li>Tutti 1 merchant ai quali altri player di circuiti di pagamento richiedono di soddisfare 1 requisiti di livello 3</li> </ul>	<ul style="list-style-type: none"> <li>Self Assessment annuale</li> </ul>	• Merchant
		<ul style="list-style-type: none"> <li>Network Scan trimestrale</li> </ul>	• Approved Scanning Vendor
Level 4	Tutti gli altri merchant che non rientrano nelle precedenti 3 categorie	<ul style="list-style-type: none"> <li>Self Assessment annuale</li> </ul>	• Merchant
		<ul style="list-style-type: none"> <li>Network Scan trimestrale</li> </ul>	* Approved Scanning Vendor /



appartenenza (merchant level); l'ultima colonna a destra definisce i requisiti per la validazione delle azioni di assessment e security scan richieste.

La fascia più "popolata" risulta la Level 2: un recente survey effettuato da Forrester Consulting in U.S. e Europa evidenzia che sull'intero campione di organizzazioni intervistate il 57% appartiene a tale categoria.

Prendendo quindi come riferimento un "merchant Level 2", il raggiungimento del "PCI Compliance status = Compliant" richiede:

- la compilazione con frequenza annuale del "PCI Self Assessment Questionnaire - SAQ", evidenziando una completa copertura dei requisiti
- l'effettuazione (con frequenza trimestrale) delle attività di Security Scan (external scan su applicazioni e sistemi Internet-facing), validate da un Qualified Scan Vendor (QSV), evidenziando l'assenza di vulnerabilità con severità di livello "High-Critical-Urgent"

Il PCI Compliance status è da considerarsi "In progress" se:

- è stato compilato con frequenza annuale il "PCI Self Assessment Questionnaire"
- sono state effettuate (con frequenza trimestrale) le attività di Network Scan validate da un QSV
- nel caso di requisiti SAQ non soddisfatti e/o presenza di vulnerabilità su applicazioni e sistemi Internet-facing) di vulnerabilità di severità di livello "High-Critical-Urgent" è stato definito ed avviato un "compliance plan", che includa la pianificazione temporale degli interventi.

Il survey citato evidenzia (vedi figura) che le aree di non-compliance si concentrano prevalentemente sulle misure di access management e di monitoring/testing.

### **Self assessment: i vantaggi di un approccio esteso**

Come indicato in precedenza, il punto focale per una compliance di livello 2 è la compilazione annuale del PCI Self Assessment Questionnaire - SAQ".

Il SAQ è articolato in funzione dei 12 requisiti base previsti dallo standard PCI, a loro volta organizzati in 6 sezioni, come descritto nella tabella seguente.

Ogni requisito è ulteriormente esploso in un set di requisiti di dettaglio di livello x.y: ad esempio il Requisito 12 "Maintain a policy that addresses Information security for employees and contractors" prevede 11 requisiti di secondo livello. Lo stato di conformità di ogni sezione è da considerarsi "GREEN" se e solo se per tutti i requisiti previsti dalla sezione risulta un "Response=YES".

L'insieme dei requisiti previsti dal SAQ non raggiunge tuttavia il livello di completezza e di dettaglio che caratterizza il set completo di requisiti PCI-DDS e le modalità di testing ad essi associati, previsti dalla procedura "Security Audit Procedures" che deve essere seguita per eseguire PCI On Site Assessment richiesto per la Level 1 Compliance; ad esempio il Requirement 12 citato in precedenza è esploso in 40 requisiti di dettaglio e relative procedure di testing.



SAQ Section	SAQ Requirement
Sect. 1: Build and maintain a Secure Network	Requirement 1: Install and maintain a firewall configuration to protect cardholder data
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Sect. 2: Protect Cardholder Data	Requirement 3: Protect stored cardholder data
	Requirement 4: Encrypt transmission of cardholder data across open, public networks
Sect. 3: Maintain a Vulnerability Management Program	Requirement 5: Use and regularly update anti-virus software or programs
	Requirement 6: Develop and maintain secure systems and applications
Sect. 4: Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need-to-know
	Requirement 6: Assign a unique ID to each person with computer access
	Requirement 9: Restrict physical access to cardholder data
Sect.6: Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data
	Requirement 11: Regularly test security systems and processes
Sect. 6: Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses Information security for employees and contractors

La verifica del livello di conformità al set di requisiti previsti del SAQ e la compilazione dello stesso rappresenta il "compitino" essenziale per la compliance Level 2. In alcuni casi i quesiti previsti dal SAQ per verificare il rispetto dei requisiti sono eccessivamente generici (ad es. il Req.1.1 chiede "Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?", e lasciano eccessivo spazio alla valutazione soggettiva dell'intervistato. E' quindi consigliabile seguire un approccio più completo, sebbene maggiormente time consuming, utilizzando l'intero set di test previsti dalla Security Audit Procedures completa: ciò richiede di mappare preventivamente ogni requisito SAQ con i requisiti PCI ed i corrispondenti test previsti dall'Audit Procedures.

Una volta completato il self assessment seguendo tale modalità estesa, rimane un problema da risolvere: assegnare un livello di conformità "YES" o "NO" ad ogni requisito SAQ, in funzione dello stato rilevato per ogni requisito PCI di dettaglio, proveniente dall'Audit Procedure, ad esso associato. Una possibile strategia si basa sull'attribuzione ad ogni requisito PCI di un peso, utilizzando un rating a due livelli: requisito mandatorio/re-quisito opzionale. Ad ogni requisito SAQ sarà attribuito un livello di conformità "YES" se e solo se tutti i requisiti PCI di dettaglio di livello "mandatario" ad esso associati sono risultati "in place".



**VALUE TEAM**

r a s s e g n a s t a m p a

### **Concludendo...**

Tale approccio consente un duplice beneficio:

1. la possibilità di identificare, oltre agli eventuali requisiti SAQ non soddisfatti e le corrispondenti azioni mandate da prevedere nel Compliance Pian, anche gli eventuali interventi atti a migliorare le modalità di implementazione delle misure di sicurezza anche laddove il requisito PCI originale SAQ risulterebbe teoricamente soddisfatto;
2. disporre di una visione completa della situazione relativa al livello di compliance rispetto al set completo di requisiti PCI, da poter riutilizzare nel caso che un incremento del numero di transazioni annue porti il livello di compliance richiesto al "Level 1", con conseguente obbligo di effettuazione di "On Site Assessment" annuali e di conformità all'intero set di requisiti PCI-DSS.