# Come scegliere il giusto QSA per la propria azienda

Quando un'azienda si trova a dover scegliente un QSA (Qualified Security Assessor) per gestire la propria conformità allo standard PCI DSS, la prima domanda che dovrebbe porsi è la seguente: *"Sto scegliendo un QSA per ottenere la compliance allo standard, o sono interessato alla sicurezza della mia azienda?"*

Se la risposta è la compliance, probabilmente sta ponendo il focus sull'obiettivo sbagliato. La conformità PCI, infatti, non è un obiettivo di business, ma un requisito normativo commerciale con un ritorno sugli investimenti minimo o nullo.

La sicurezza, invece, se viene gestita correttamente, è un abilitatore del business e, una azienda che punta a proteggere i propri dati critici, i controlli previsti dallo standard PCI DSS dovrebbe averli già implementati.

La scelta del giusto QSA non deve pertanto essere mirata al semplice ottenimento della certificazione, ma dovrebbe portare a selezionare un esperto di sicurezza che sappia interpretare lo standard PCI DSS per adattarlo al contesto operativo dell'azienda, ed aiutarla ad implementare le misure di sicurezza più idonee a proteggere il business aziendale.

Di seguito sono riportate le domande più rilevanti che una azienda dovrebbe porre ai potenziali QSA per scegliere quello più adatto a gestire il proprio piano di compliance, con l'obiettivo di non scegliere necessariamente il più grande, il più economico o quello più vicino in termini di posizione geografica, ma di selezionare il QSA che effettivamente sia in grado di aiutare l'azienda a raggiungere un livello di sicurezza adeguato per i propri obiettivi di business.

# Come si colloca lo standard PCI DSS rispetto ad altri standard di sicurezza?

Prima di vedere in dettaglio le domande che una azienda dovrebbe porre ai potenziali QSA per scegliere quello più appropriato al proprio business, è importante vedere come si colloca lo standard PCI DSS rispetto ad altri standard di sicurezza o alle Security Good Practice.

Ad un livello molto alto, un programma di sicurezza è costituito dai seguenti elementi:

| **Elementi del programma di sicurezza** | **Security Good Practice[1]** | **ISO/IEC 27001** | **COBIT** | **PCI DSS** |
|---|---|---|---|---|
| Revisione del Business Plan / Definizione degli obiettivi di sicurezza | X | | X | |
| IT Risk Assessment | X | X | | X |
| Business Impact Analysis | X | X | | |
| Formalizzazione di Policy o Procedure | X | X | X | X |
| Implementazione dei controlli di sicurezza | X | | | X |
| Implementazione di un Sistema di Gestione della sicurezza | X | X | | |
| Istituzione di un comitato per la Governance della sicurezza | X | | X | |
| Integrazione di un piano di Change Control | X | X | | X |

| | | | | |
|---|---|---|---|---|
| Disaster Recovery e Business Continuity | X | X | | |
| Implementazione del ciclo di vita della sicurezza (Plan, Do, Check, Act) | X | X | X | |
| Gestione della sicurezza nei processi Business as Usual | X | | | |

Osservando le voci elencate nella tabella, è possibile affermare che:

- A meno che non si sappia cosa vuole l'azienda e come funziona, non è possibile progettare un programma di sicurezza adeguato;
- Senza un IT Risk Assessment e una Business Impact Analysis, non si riesce a sapere quali dati sono davvero importanti per l'azienda e non è possibile definire un budget appropriato per l'implementazione del programma;
- Verranno implementati solo i controlli che sono in linea con la valutazione del rischio, indipendentemente dalla compliance;
- L'implementazione dei controlli di sicurezza senza un sistema di gestione che li mantenga allineati all'evoluzione dei processi aziendali non supporta né la sicurezza né la compliance;
- La Governance e il Change Management vanno di pari passo, e influenzano le comunicazioni tra il business e l'IT, a garanzia del mantenimento della compliance;
- La compliance e la sicurezza sono prive di significato se non si rivolgono al business aziendale, integrandosi con l'operatività "Business as Usual" dell'azienda;
- I passaggi precedenti non sono lineari, ma ciclici e continui nel tempo.

# Quali domande porre al QSA per selezionare quello giusto

Di seguito sono riportate le domande pensate per la scelta del QSA. Sono domande abbastanza generiche, in modo che possano adattarsi a qualsiasi contesto aziendale.

1. **Da quanto tempo svolge le attività di QSA?**

Una società che opera come QSA da pochi mesi è più a rischio di una che è attiva da un decennio, soprattutto per un progetto a lungo termine come quello di acquisire la certificazione PCI DSS per la prima volta.

Questo non vuol dire che dovrebbero essere escluse automaticamente tutte le nuove società che si affacciano sul mercato, ma in tal caso sarebbe opportuno valutare se forniscono solo i servizi di certificazione PCI, oppure se la PCI è solo una parte della loro offerta consolidata di servizi di consulenza sulla sicurezza.

2. **Da quanto tempo svolge security assessment, inclusi gli assessment PCI?**

Una società che esegue security assessment da poco tempo potrebbe non avere l'esperienza adeguata per eseguire in modo efficace un assessment PCI, a meno che non abbia personale con molta esperienza pregressa come QSA.

Nello standard PCI DSS i controlli sono una parte molto importante di un framework di sicurezza, ma non l'unica. Per questo, la prima domanda che dovrebbe porre un QSA non è "***dov'è il diagramma di rete?***" ma piuttosto "***dov'è la valutazione del rischio?***".

3. **Quanti dei suoi consulenti QSA hanno sottomesso un Report on Compliance?**

Sebbene sia piuttosto semplice per un consulente diventare QSA

(5 anni di esperienza sulla sicurezza, essere in possesso di alcune certificazioni ecc.), questo non significa che un QSA sia effettivamente qualificato per eseguire un assessment e fornire una guida alla gestione della sicurezza in un ambiente complesso.

Chiunque può mettere in evidenza le cose fatte in modo sbagliato che rendono l'azienda non compliant, ma per fornire indicazioni su cosa fare al riguardo e superare la non conformità serve un consulente QSA di provata esperienza.

Se il personale della società QSA ha maturato esperienze nella sottomissione dei Report on Compliance al Security Standard Council, allora ci sono buone probabilità che sappia affrontare nel modo giusto un progetto complesso di certificazione.

4. **Quanti Report on Compliance ha presentato?**

Come per il punto precedente, tanti più RoC sono stati presentati maggiori garanzie ci sono che la società abbia sviluppato processi interni standard per eseguire gli assessment e processi di quality assurance a garanzia delle attività svolte.

Ancora una volta, questo non dovrebbe automaticamente precludere l'acceso alle nuove società QSA che si presentano sul mercato, ma è a garanzia dell'adozione di standard di qualità elevati.

5. **Quanti assessment ha eseguito presso altri clienti che svolgono le stesse attività dell'azienda, o che operano nello stesso settore?**

Eseguire un assessment su di un *merchant* è molto diverso dall'esecuzione di un assessment su di un *service provider* o su un *acquirer / issuer*.

Se il QSA non ha mai eseguito assessment su clienti che

svolgono lo stesso tipo di attività dell'azienda, probabilmente non offrirà un servizio di qualità, e potrebbe potenzialmente generare problemi o extra costi.

Viene chiesto quanti assessment ha eseguito la società, e non il singolo QSA, perché tipicamente un assessement non viene mai eseguito da un solo QSA. Un singolo consulente, infatti, non ha le competenze necessarie per valutare adeguatamente lo stato di conformità di una azienda su tutti i 12 domini dello standard PCI.

Ogni valutatore ha una competenza unica, quindi la scelta del QSA dovrebbe portare a preferire una società con un sufficiente mix di competenze dei consulenti per coprire tutte le proprie esigenze.

6. **In che modo garantisce la continuità di una attività di assessement?**

L'obiettivo di questa domanda è quello di verificare in che modo è organizzato il processo di assessment, in modo tale da garantire che tutte le informazioni siano sempre immediatamente disponibili a tutto il team di lavoro secondo una metodologia consolidata e collaudata.

La sostituzione di un QSA a metà di un assessement è uno dei problemi più grandi che una azienda può trovarsi ad affrontare nella gestione di un processo di certificazione, anche se si tratta di un consulente diverso che lavora per la stessa società QSA.

In tali casi, la società QSA deve assicurare che eventuali cambiamenti del team non abbiamo impatti sui tempi di conseguimento della certificazione e non richiedano ulteriori costi.

7. **Come vengono gestite eventuali divergenze di valutazione dei QSA che fanno parte dello stesso team di lavoro?**

Questa domanda è finalizzata ad approfondire la maturità e l'esperienza dei QSA che svolgono le attività di assessment e dell'azienda QSA nel suo complesso.

Lo standard PCI DSS è aperto ad una grande quantità di interpretazioni (si veda ad esempio la definizione di "periodico" o di "appropriato"), quindi qualsiasi decisione presa da un QSA deve essere condivisa da tutto il team di audit e formalizzata della società, in particolare laddove vengono individuati effort significativi per raggiungere la conformità, sia in termini di costi di che di risorse.

8. **Sono previsti degli SLA per la comunicazione e la risposta alle domande poste dall'azienda?**

Non c'è niente di più frustrante del fatto che il punto di contatto presso il QSA non risponda alle richieste che gli vengono rivolte dall'azienda. Per questo motivo, sarebbe opportuno che nel contratto con il QSA fosse presente uno SLA sui tempi di risposa.

9. **La società fornisce altri servizi di consulenza relativi alla compliance o alla sicurezza?**

Lo standard PCI DSS è rivolto specificamente al trattamento dei dati dei titolari di carta e non copre la conformità o le esigenze di sicurezza che potrebbe avere una azienda rispetto ad altri ambiti (dati personali, dati finanziari, proprietà intellettuale, ecc.).

Nella scelta di un QSA, una azienda dovrebbe assicurarsi che la società abbia anche l'esperienza necessaria per trattare altre categorie di dati, o altre normative alle quali l'azienda deve rispondere (es. GDPR, SOX, ecc.) al fine di ottimizzare gli investimenti ed avere un interlocutore unico per tutte le tematiche di sicurezza.

10. **La società può consigliare prodotti o servizi che possano aiutare a raggiungere la conformità?**

Per alcune società QSA, la consulenza PCI è solo una mezzo per vendere un insieme di ulteriori prodotti o servizi per "aiutare" l'azienda a raggiungere o a mantenere la conformità allo standard.

E' molto importante capire se il QSA è una società di servizi nata per fornire una guida imparziale ed esperta per il conseguimento della certificazione o è una società di prodotti travestita da QSA.

Per il Security Standard Council, ad esempio, è accettabile per una singola società:

- vendere un firewall;
- gestire e manutenere un firewall;
- eseguire il monitoraggio di un firewall;
- eseguire una scansione di vulnerabilità o il penetration test di un firewall;
- valutare la conformità PCI di un firewall.

Questo, tuttavia, potrebbe generare un conflitto di interessi, portando probabilmente a violare le Policy di Sicurezza aziendali e tutte le Good Practices di gestione della sicurezza.

Se oltre alla consulenza sulla PCI la società offre anche servizi di sicurezza gestita, deve assicurare che i servizi offerti supportino la compliance dell'azienda. Questi servizi dovrebbero essere inoltre sottoposti ad assessment indipendenti, e dovrebbero essi stessi ottenere una certificazione PCI.

11. **Come può supportare l'azienda a mantenere la certificazione nel tempo?**

Una volta raggiunta la certificazione, questa deve essere mantenuta nel tempo. Per questo, come parte di un servizio di consulenza, il QSA dovrebbe aiutare l'azienda a definire un programma di sicurezza e ad implementarlo a livello aziendale.

12. **Se non è possibile soddisfare esattamente tutti i requisiti previsti dallo standard, cosa succede?**

Nessun soggetto è conforme esattamente a tutti i requisiti dello standard PCI punto per punto.

Laddove non è possibile soddisfare a pieno i requisiti dello standard, devono essere messi in atto dei controlli compensativi che garantiscano gli stessi livelli di sicurezza dei controlli dello standard.

Un buon QSA è a conoscenza di tutti i principali controlli compensativi che sono stati accettati dal Security Standard Council ed è in grado di supportare al meglio un'azienda mettendo a disposizione la propria esperienza e le proprie conoscenze.

Per questo è fondamentale che venga scelto un QSA che sia prima di tutto in grado di mettere a disposizione dei consulenti, e non solo degli auditor.

13. **Come scegliere il migliore QSA?**

Al fine di scegliere il migliore QSA, sarebbe opportuno mettere a confronto almeno due potenziali candidati, ponendo domande puntuali relative alla certificazione del proprio contesto aziendale. Se le risposte fornite non sono esaustive, è bene continuare con la selezione.

14. **Dove è possibile ottenere un elenco di tutti i QSA?**

Un elenco completo di tutte le società QSA è disponibile al seguente link: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

15. **Quanto ci vuole per ottenere la certificazione PCI?**

È impossibile rispondere a questa domanda senza ulteriori informazioni sull'azienda da certificare. Un QSA che

garantisce la certificazione in un arco temporale senza conoscere il contesto dell'azienda, andrebbe escluso dalla scelta.

## Conclusioni

La scelta di un QSA può sembrare scoraggiante, specialmente per una azienda che non dispone al proprio interno di uno specialista di sicurezza. Tuttavia, se si tengono in considerazione le domande elencate è possibile scegliere il miglior QSA per i propri obiettivi di business.

Ed è bene ricordare che:

- La PCI DSS riguarda la protezione dei dati dei titolari di carta e non copre tutti gli aspetti di compliance di un'azienda;
- La PCI non è (da sola) una Good Practice di sicurezza, ma costituisce un insieme di "controlli di sicurezza" ritenuti sufficienti dai brand delle carte di pagamento;
- Un progetto per ottenere la certificazione allo standard PCI dovrebbe essere avviato solo dopo aver eseguito un IT Risk Assessment e una Business Impact Analysis;
- La prima fase per avviare un progetto di certificazione PCI deve riguardare l'individuazione dello *scope* di certificazione;
- L'implementazione dei controlli previsti dalla PCI senza un sistema di gestione per mantenerli, non garantisce né la sicurezza né la compliance;
- Un buon QSA è in grado di interpretare i requisiti della PCI affinché possano garantire effettivamente un innalzamento del livello di sicurezza dell'azienda.

[1] https://www.securityforum.org/tool/the-isf-standardrmation-security/

A cura di: **Francesco Morini** e **Fabio Pacchiarotti**

L’articolo Come scegliere il giusto QSA per la propria azienda proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/come-scegliere-il-giusto-qsa-per-la-propria-azienda/