CORE
CONCEPT
SECURITY

Selecting the Right QSA for Your Business

May 2013

CONTENTS

EXECUTIVE SUMMARY

PCI has been around for years, yet I've seen very few papers on how to choose the right QSA for your business. At least not ones that are aren't completely biased. You would think both the card brands and the SSC would want to help you achieve compliance in line with your business needs, as well as ensure that the QSA companies providing these services have met, and continue to meet, the standard of service expected.

Well, they actually do, but their hands are somewhat tied. Any attempt to provide this guidance would automatically exclude several QSA organisations who cannot adequately meet some, and in a few case any, of the criteria below. A good thing you might say, but it also stifles competition. With the right due diligence in place, separating the wheat from the chaff is actually a fairly simple process.

Having been a QSA for as long as there have been QSAs, as well as being in a position to be as objective as I can ever be, I thought I'd try my hand at providing some of this guidance.

ADDRESSING THE CHALLENGE

First, you must ask *yourself* one question; “Are you choosing a QSA *just* to be PCI compliant, or do you actually care about security?”

If the answer is compliance, you're probably starting out with the wrong goal in mind. PCI compliance is not a business goal, it's a commercial regulatory requirement with little to no return on investment, or positive impact to the security of your whole business.

Security done correctly is a business enabler, and every one of the PCI controls should *already* be in place if you want to protect your sensitive data to even a minimum standard.

> *“Remove the phrase 'cardholder data' from the PCI DSS and replace it with 'personal information about your family'.*
>
> *Name one requirement you would not want in place?...”*

The right QSA is a security expert first and foremost, and knows how to fit PCI compliance into your *existing* business goals. You should have these goals in mind before you start working on compliance for your investment to make sense.

Below are what I believe to be the most relevant questions to ask prospective QSA companies up front. Don't just go with the biggest, the cheapest, or the closest in terms of geographic location, choose the one who will actually help you meet your business goals. Or even better, one who can help you *define* appropriate goals if you don't have any.

WHAT IS SECURITY?

Before the questions you ask the candidate QSAs will make any sense, we must first put PCI into a little perspective. And you as the reader will need to accept, with maybe a few personal amendments, my description of a security program done correctly.

At a very high level, a security program will contain all of the following steps;

Security Program Elements	PCI	ISO	COBIT	SGP*
Review Business Plan / Goals			✓	✓
Risk Assessment	✓	✓		✓
Business Impact Analysis		✓		✓
Policy & Procedure Formalisation	✓	✓	✓	✓
Security Control Implementation	✓			✓
Management Systems Implementation		✓		✓
Hand-off to Governance Committee			✓	✓
Change Control Integration	✓	✓		✓
Disaster Recovery & Business Continuity		✓		✓
Initiate Information Security Life Cycle**		✓	✓	✓
Begin Business As Usual				✓

* Security Good Practices ** Plan > Do > Check > Act > Repeat

Assumptions

1. Unless you know what the business wants, and HOW it does business, you cannot design an appropriate security program;
2. Without a Risk Assessment and Business Impact Analysis, you have no idea what your data is worth, and cannot define an appropriate budget;
3. You will implement ONLY those controls that are in line with the risk assessment, regardless of compliance;
4. Security Controls without management systems to KEEP them in place will support neither security, nor compliance;
5. Governance and change control go hand in hand, and effect business-to-IT communications and continuous compliance respectively;
6. Compliance and security are meaningless if you don't stay in business, so DR and IR all feed into Business Continuity Planning and Business as Usual; and
7. The above steps are non-linear, cyclical, and never ending

THAT DETECTIVE, IS THE RIGHT QUESTION…

The questions below are designed to be generic enough to suit almost any business, as well as form the core questions in your Request for Proposal (RFP);

1. *How long has your company been in business?*

   A company that has been in business for only a few months is a higher risk than one that's been in business for a decade, especially for a long-term project such as achieving PCI compliance for the first time. That's not to say you should automatically exclude new businesses (they have to start somewhere), but do they ONLY provide PCI services? If yes, there's a good chance they jumped on the PCI budget bandwagon. If you do choose a new business, make sure that PCI is only a small part of their security consulting service offerings (see point 2 below).

2. *How long has your company performed security assessments, including PCI?*

   Notice I say "including" PCI, as this is not the only service they should be providing. The controls in the PCI DSS are only one part of an effective and overarching security framework (See 'What is Security?' above). A very important part yes, but even these minimal controls should be deemed appropriate before spending significant time and money implementing them. The first question out of your assessors mouth should not be "Where's your network diagram?", it should be "Where's your Risk Assessment?".

   Also, unless companies are formed by experience QSAs, they may not have the experience to perform the assessment efficiently.

3. *How many of your QSAs have submitted a compliant Report on Compliance?*

   It is depressingly easy to become a QSA. While you do have to show 5 years of security-relevant experience, and CISSP/CISM/CISA [et al] qualifications to qualify for the training, none of this means you're actually qualified to provide real world security guidance. The SSC's QSA training is far too easy, and does not separate the auditors from the consultants. Anyone can tell you what you're NOT doing to be complaint, it's written down for you, but it takes a consultant with experience to provide guidance on what to do about it if you aren't.

   If the consulting staff of the QSA company are experience in submitting reports to the SSC, there's a far better chance that they can eventually do so on your behalf.

4. *How many Reports on Compliance has your company submitted?*

   As per number 3 above, the more the better, as it speaks to the necessity to standardise both the assessment and the quality assurance processes.

   Again, this should not automatically preclude newer QSA organisations as long as the consultants working for that company are appropriately experienced.

5. *How many assessments has your company performed in my business type / industry sector?*

Performing an assessment on a level 1 merchant is very different than performing an assessment on a level 1 service provider, or an acquirer / issuer. Unless the QSA has actually performed assessments on your type of business, the service will likely be flawed, potentially causing significant and costly issues down the road.

The reason I ask how many assessments the company has performed, and not the individual QSAs is because an assessment should not be performed by a single QSA alone. Yes, you may have a singly focal point / point of contact, but no single consultant has the necessary skills to assess your business adequately against all 12 PCI requirements. Every assessor has a unique skill-set, so your QSA company of choice should have a sufficient mix of skill-sets to cover your entire organisational needs.

6. *How do you maintain the continuity of an engagement?*

This is by far the biggest complaint of every organisation which has had to replace a QSA mid assessment, even if it's a different QSA working for the same QSA company. How do you maintain the continuity of the assessment process when there is so much information in the departing assessors' head? Does all of that knowledge go with them, or is the assessment process itself so well organised that the information is ready to hand? Unless you are satisfied that the assessment process is backed by a tried and tested methodology, this unfortunate (but frequent) issue may raise its ugly head. At the very least ensure that any time spent bringing the new QSA up to speed is at the QSA company's expense, not yours, as the ensuing delays can be extensive.

7. *How do you deal with the differing opinions of your QSAs?*

This question speaks to consistency, as well as the experience of both the individual QSAs, and the maturity of the QSA company as a whole. Bottom line; any opinion from any QSA should have the backing of their organisation, especially where significant capital or resource costs expenditure is required. The PCI DSS itself is actually open to a great deal of interpretation (define 'periodic', or 'appropriate' for example?), so any decisions made by one QSA must be agreed by them all.

Unless the QSA company has a formal process for accepting their QSAs decisions, in writing, and backed by contract language, you'll want to keep looking.

While this does not help you maintain consistency from one QSA company to the next, you can be assured that the more experienced QSAs have already had their opinions previously supported.

8. *Do you have communication SLAs?*

The is nothing more frustrating than having your point of contact resemble a black hole to your communication attempts. Have reasonable expectations, but insist that an SLA be built into your contract.

For example; An acknowledgement of receipt for all communication to be received within 1 business day.

9. *Do you provide any other compliance or security related consulting services?*

PCI is very specific to cardholder data. Too specific in fact to cover the compliance or security needs of all the sensitive data types you have in your systems. Do you have personal data? Financial data? Intellectual property? Spending money on PCI and not including ALL of your businesses sensitive data is probably not the best use of your budget.

In choosing a QSA, make sure that they have the necessary experience in dealing with other forms of data which may be covered by non-PCI regulatory or compliance standards (the EU Data Protection Directive, PoPI in SA, or HIPAA in the US for example.)

10. *Can you recommend products or services to help us achieve compliance?*

Be very careful here. For a lot of QSA companies, the PCI consulting is just a means to an end, and that end generally involves selling you a bunch of their OTHER products or services to 'help' you achieve compliance.

Review their website carefully, what are you first impressions? Are they a service company designed to provide impartial and expert guidance, or are they a product company disguising themselves as a QSA to get you to buy more stuff?

As far as the SSC and the card brands are concerned, it is perfectly acceptable for a single organisation to (for example);

- Sell you a firewall;
- Manage and maintain the firewall;
- Monitor the firewall;
- Scan and pen test the firewall, AND;
- Assess the firewall for PCI compliance

This may make sense for your organisation, but even common sense suggests this is very likely a conflict of interest. Your vendor program may be easier to maintain, but does this complete absence of checks and balances fit with your security policy, or any known security good practice?

The answer to this comes back to your view on PCI itself; are you doing this for compliance, or security?

If you do combine your PCI consultancy with a managed service from the same organisation, make sure their services support your compliance. Preferably, these services will have been independently assessed, and have achieved PCI certification.

Last warning about security managed services; have your provider, or prospective providers detail EXACTLY which of the PCI DSS requirements they cover, and to what extent. A lot can be hidden from you if you make assumptions.

11. How do we maintain PCI compliance?

So you've achieved compliance, now what? All compliance means is that at a SINGLE point in time over the last year the controls were in place on a SAMPLE of your systems. It does not mean that these controls were in place on all of the systems, all the time.

PCI compliance without some form of management systems in place as a wrapper around them is almost pointless. You are no more secure than you were before, and you will probably have to expend the exact same effort to re-certify your compliance as you did achieving it in the first place.

As part of a good consulting service, your QSA should at least have a plan to help you take your PCI program and develop it into an enterprise-wide security framework. Whether you choose this route or not, you should at least have the 'plug-ins' to do it later.

12. If we cannot meet every regulatory requirement exactly, then what?

No-one is PCI compliant exactly per the requirements, period/full-stop. It's impossible, and unnecessary. However, seeing as the PCI controls are a minimum standard, it should be every organisations' goal to get as close as possible without exceeding the value of the data itself. You will know where that balance is if you do your Risk Assessment properly.

Compensating controls are a fact of life, and the only way to fit the previously rigid black and white controls of the DSS into your business. It should never be the other way around.

The best QSAs have a database of compensating controls that have been accepted both by the QSA company as a whole, and by the SSC or card brand (depending on your business type). This guidance should be available to you immediately, as should several mitigating options which can be tailored to your specific needs.

There is no room for black and white interpretation in security, PCI cannot be any different. Choose a QSA with a similar outlook, and one who employs only consultants, not auditors.

13. What is the security experience of your QSA?

Insist on interviewing a couple of the potential QSAs per company, have a list of questions most important to YOUR business ready. If you don't like the answers, or if the candidates do not give you the warm and fuzzies, move on.

They do not have to know the answer to all of your questions, but they do have to be completely up front with you. It's OK not to know something as long as you know someone who does. That's what consultancy is; knowing where to get the answers.

14. Where do I get a list of potential QSA companies?

For a full listing of all QSA companies, visit the link, below, then choose a good cross section of organisations that do business in your region;

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

15. How long does it take to get compliant?

Impossible to answer without a LOT more information. Immediately dismiss any QSA company that gives you an up-front timeframe unless all you care about is getting certified, and not actually achieving proper compliance.

This a 'trick' question designed to weed out the worst offenders.

SUMMARY

Choosing a QSA can seem daunting, especially if you do not have a security specialist on staff. However, if you keep the following points in mind, and ask all the questions above, you should be able to choose the best QSA for your business goals;

1. PCI DSS is not about compliance, it's about securing cardholder data to the card brands' satisfaction;
2. PCI is not (by itself) a good security practice, it is 'security controls enough' for the card brands (but not necessarily for your business);
3. A PCI 'project' conducted outside of existing business process / risk management program could be a waste of time and money;
4. PCI controls without the management systems to maintain them, will not keep the data secure, let alone keep you compliant;
5. Don't start PCI until you have done a Risk Assessment, a Business Impact Analysis, AND a scoping exercise; and most importantly
6. PCI must fit into your business, not the other way around!

Best of luck!

ABOUT FROUD

David has almost 20 years of experience in areas of Information / Cybersecurity, including Regulatory Compliance, Secure Architecture Design, Governance Frameworks, Data Privacy & Protection, and FinTech.

As Project Lead for several Fortune / FTSE 'Enterprise Class' clients, David has performed hundreds of on-site PCI, security, and regulatory compliance assessments for organisations globally.

Blog: http://www.davidfroud.com

Linkedin: http://www.linkedin.com/in/davidfroud

ABOUT CORE CONCEPT SECURITY

Core Concept Security (CCS) is an independent cybersecurity and data protection consulting practice based in the UK, but available globally.

The guiding principle behind all CCS's services is that security, while often difficult to achieve, has always been, and will always be, simple. There are no shortcuts to security, and there is nothing to be gained by just throwing money at it hoping the problems will go away. Technology will never fix what's broken, only people and process can.

The CCS approach is also simple; It's our job to help you ask the right questions, even if we aren't the ones who can actually answer them. You're hiring us, you're hiring everyone we know.

In the end, if your security program is not appropriate to your business needs it is a waste of your time and effort. Our commitment to our customers is to never settle for less than, or try to sell you anything *more* than, what you need.