SECURITYRISK ADVISORS

Web: www.securityriskadvisors.com
Email: info@securityriskadvisors.com
Twitter: @secrisk

OUR VIEW ON THE LATEST SECURITY ISSUES AFFECTING OUR CLIENTS

ThreatView

August 2012

"The approach you select should focus on the most effective way to mitigate the risk of a credit card breach in your organization"

Benefits of adding an ISA to your PCI Compliance Program

When the Payment Card Industry Data Security Standard (PCI DSS) became a required framework in 2006 for all merchants who accepted credit cards, many different approaches to PCI DSS compliance emerged and have evolved since then. In the beginning, the Qualified Security Assessor (QSA) approach was *recommended* by the PCI Security Standard Council, however never *required*. This resulted in a number of Level 1 merchants opting to 'self-assess' their PCI posture as they felt this approach better fit into their organization. However, in 2009 MasterCard introduced changes to their Site Data Protection (SDP) program that required all Level 1 and Level 2 merchants to use a QSA to meet the PCI compliance validation requirements.

This caused uproar within the industry, in particular for those merchants who already spent time and resources developing an internal program. MasterCard listened and the compromise was the creation of the Internal Security Assessor (ISA) program. This gave merchants an option to certify employees within their organization to validate their PCI compliance. This brought back the option to 'self-assess' while giving the card brands more comfort over the quality and consistency of these programs. This ISA option is now available to Level 1 merchants completing a Report on Compliance (ROC) or Level 2 merchants completing the appropriate Self-Assessment Questionnaire (SAQ) for their organization.

This ThreatView begins by contrasting the benefits and potential downsides of an exclusive QSA or ISA approach. We then introduce some questions which can aid your decision process, and illustrate through two examples how a Hybrid QSA+ISA approach can sometimes provide the best overall risk management benefit.

So what are the pros and cons of QSA and ISA?

	Pros	Cons
QSA	✓ Independent attestation of PCI validation, free of internal disagreements ✓ Expertise your organization may not have internally ✓ Obtain recommendations based on experience working with other companies like yours	✓ Quality of individual QSA auditor work can vary with individual background and experience ✓ Program can slip towards passing an audit vs. managing risk of a breach ✓ Still requires internal staff to facilitate QSA requests ✓ No liability for QSA in event of breach – it's still on you

	Pros	Cons
ISA	✓ "Ongoing" approach to compliance efforts can result in better-sustained risk management ✓ Create strong relationships between ISA program and system/process owners ✓ Not subject to a third parties' interpretation of PCI Requirements ✓ Ability to integrate other compliance programs	✓ No outside perspective built-in to the process ✓ Skillset required to manage a PCI program not always readily available within organization ✓ Not an option for Level 3 or 4 merchants

We've seen some significant benefit from combining the best of both QSA and ISA into a Hybrid approach. However, it is important to note that the "cons" of an exclusive QSA or ISA model can be managed; it is still viable to use those approaches so long as your program can avoid certain pitfalls. Before you decide whether to modify your current approach consider the following:

- What is the payment channel, process and system scope of my organization's PCI Environment?
- How many dedicated internal resources are required and how many more could be made available to contribute to the program?
- Does my organization possess the skillsets to manage technical and/or process-oriented validation procedures?
- Can I integrate my program with an existing compliance function and leverage existing resources (e.g. – SOX, GLBA, HIPAA)?
- Does my scope change often enough such that I need to monitor the applicability of my controls on a frequent basis?
- If I were to consider a Hybrid model, which benefits (the "pros" in both columns) would we be able to take advantage of? Which "cons" would it help us minimize?

We've included two sample scenarios to illustrate the thought process of how some merchants benefit from a Hybrid approach:

Merchant:	***HotTickets***
Merchant Level:	Level 2
Validation:	SAQ D
Background:	HotTickets is an e-commerce business that sells tickets to live music and sporting events. Most purchases are sent directly from their website to their payment processor; however they do store cardholder numbers to provide a "future payments" option to their customers. HotTickets has a small staff of 500 employees. They do not have other regulations to consider within their environment, and do not have a dedicated compliance function. Although their website is updated on a monthly basis, they have a defined software development lifecycle and have gone through an audit performed by their security team to ensure the PCI DSS requirements are addressed.
Approach:	Although HotTickets has confidence in their security team, they decided they would be more comfortable with a third party attesting to their scope and assessment. HotTickets also opted to certify one of their employees under the ISA program and decided to use a QSA annually to perform an audit and validation of their environment. HotTickets' ISA is a part-time role. The main purpose of the ISA role is to assess and communicate how business decisions may affect the scope of the PCI program.

Merchant:	***CityWide Healthcare***
Merchant Level:	Level 1
Validation:	Report on Compliance
Background:	Citywide Healthcare provides patient services through their network of hospitals and doctor offices. They accept credit cards as a form of payment in person at their hospitals and offices, through their website, over the phone and through an Interactive Voice Response (IVR) system. These systems are separate and managed by different teams. The business processes for accepting credit card payments are not standardized across the various payment channels. Citywide Healthcare has over 50,000 employees. They have invested in central internal audit and compliance departments to support a number of government regulations they are required to meet. Citywide Healthcare has grown in large part due to acquisition, resulting in difficulty maintain regulatory compliance across the company.
Decided Approach:	CityWide Healthcare knew they had more complex cardholder environment than many merchants, not to mention a business culture rife with hurdles to effect change. CityWide Healthcare decided to use a hybrid approach that involved concurrently using an external QSA while training their staff to become ISA certified. This approach provided them assurance that their program was appropriately addressing the PCI DSS requirements while ensuring their internal groups could maintain the program in the long run. CityWide Healthcare understood that to maintain PCI compliance, a long term investment in internal relationships would need to be made.

Summary

Many organizations view PCI as another project for IT audit that needs to be completed in order to avoid fines and remain in good standing with their acquiring bank and the card brands. While there is some truth in that, the underlying intent of PCI DSS is to prevent your organization from suffering a breach which can result in the loss of cardholder data and loss of customer confidence. Why bother to contrast compliance with breach risk? The approach you select should focus on the most effective way to mitigate the risk of a credit card breach in your organization, with less emphasis on meeting the letter of the law for all the PCI requirements.

Contact Us

Your environment probably has similarities to the many we've seen and worked in, but is likely unique and complex in its own way. Contact us, we'd be happy to talk about it and share perspective.

Carl Angeloff
carl.angeloff@securityriskadvisors.com
412.974.3333

Carl has consulted on all things PCI with Fortune 500 clients and himself served as an ISA for a Fortune 50 company prior to joining Security Risk Advisors. As Compliance Services Lead, Carl specializes in PCI strategy, scope reduction and remediation.

Tim Wainwright
tim.wainwright@securityriskadvisors.com
215.901.4905

Tim is Client Service Lead at Security Risk Advisors. He has consulted on PCI strategy, data protection (including DLP implementation and effectiveness), technical security assessments, customer and enteprise mobile security