

PCI DSS Pre-assessment:

Managing the process to limit liability

Remember all the things you used to do in college to prepare for final exams? You took preparation quizzes and reviewed only the topics you knew would be on the exam, and you usually passed. Preparing for a Payment Card Industry Data Security Standard (PCI DSS) audit is not that different. But in the real world, you may be tested on items that aren't on the exam. Remember, it's ultimately to your benefit to pass a PCI audit.

As a part of the compliance process, most Level 1 merchants will conduct a pre-assessment audit prior to the official PCI audit to discover and remediate problems before they turn up in the real audit. These pre-assessments not only help build a baseline to ensure that compliance is achieved as efficiently as possible, but can also highlight findings that may be a liability for the company if not handled properly.

This tip will briefly outline the pre-assessment process and explain what to do when less-than-desirable results turn up.

The pre-assessment process explained....

Performing a pre-assessment prior to the anticipated visit of the PCI Qualified Security Assessor (QSA) is an extremely valuable exercise. The pre-assessment will help an organization identify and learn about existing gaps between its current security posture and the PCI DSS. In addition, it will provide a head start for organizations in remediating identified gaps prior to the official PCI audit.

In planning a pre-assessment audit, there are a number of factors that need to be considered. First, determine the PCI level the issuing bank has assigned to your organization. This level is based on the volume of transactions that occur over a certain time period. Identifying your level will assist in developing the appropriate breadth and depth of the pre-assessment engagement. Next, you will want to schedule enough time to allow for your organization to internalize the findings and complete the remediation work. Additionally, factors such as the number of systems and processes to review and the depth of testing can be used to estimate the time and cost associated with the pre-assessment activity.

The process of selecting the right partner to conduct a pre-assessment is also critical. Many businesses will look for a trusted advisor to assist in translating the risks to the executive team in order to make the most cost efficient decisions. Other businesses will want to change third-party auditors each year to have variations in approach and, thereby, variations in potential findings. No matter which method works best for your organization, the services offered by a third-party auditor should include on-site reviews of IT infrastructure, network design, application architecture and policies. Upon concluding the pre-assessment audit, an initial gap analysis and recommendations report should be provided to define the scope, findings and prioritization of remediation activities.

Once a pre-assessment is conducted and the pre-assessment team validates the findings, they must be presented and understood by the executive team. Executives are ultimately responsible for correcting or mitigating issues identified in the pre-assessment. Conversely, if the executive team chooses to accept certain risks instead of taking corrective action, the analysis and decisions have to be documented, in case PCI auditors later note a discrepancy about any control objectives.

PCI DSS Pre-assessment: Managing the process to limit liability

Managing pre-assessment findings

Even with a pre-assessment, there are important legal considerations to plan for. A best practice is to start by officially asking your organization's legal team for advice on conducting a pre-assessment. Make sure the legal team is involved at an early stage -- prior to having any discussions with third-party companies -- to ensure that the final results will be protected appropriately, namely from future discovery requests that may reflect negatively on your organization or its security posture. For example, the legal team may position items so that they hire the third party to aid in the legal work. By doing so, the producer of the pre-assessment results will report directly to the legal team confidentially and can be protected from future discovery.

Failing to protect pre-assessment results early in the process can have dire results at a later date. For instance, if the company is involved in litigation involving a breach or identity theft, a discovery request may cause the results to wind up as "exhibit A" in a future lawsuit.

After pre-assessment remediation

Based on the final outcome of the pre-assessment and the remediation work identified and completed, the internal legal team would have the opportunity to extend the protection of the pre-assessment findings. This will allow your organization to determine if the pre-assessment findings would be made available to the PCI auditors during the official audit.

Without question, a company puts itself in the best possible position to manage pre-assessment results, both in the short term and the long term, by including the legal team from the earliest stages of the process. You will discover that your PCI compliance objectives can be met and the legal liability to the company can be kept in check while building better compliance life cycle management into the process.

ABOUT TBG SECURITY

TBG Security provides compliance services the Fortune 1000, as well as other leading retail, education, healthcare and telecommunications companies. TBG Security is engaged by leading companies around the world, including: Partners Healthcare, Bahamas Telecommunications Company, US Fiduciary Service and more. TBG Security Compliance Services provides a complete spectrum of compliance management consulting and integration services, including payment service integration, risk management compliance administration, automation and payment security compliance.