

## PCI Quality Assurance Program Does Not Go Far Enough

John Pescatore, Avivah Litan

The Payment Card Industry's new quality assurance program will do nothing to address the industry's most serious compliance problem: the conflict of interest inherent in assessors' also performing remediation.

## NEWS ANALYSIS

---

### Event

On 17 November 2008, the Payment Card Industry (PCI) Security Standards Council (SSC) introduced a program to monitor the performance of consulting firms certified as qualified security assessors (QSAs) permitted to evaluate merchant compliance with the PCI Data Security Standard (DSS). The program will require QSAs and their employees to:

- Adhere to PCI SSC validation requirements
- Maintain consistent assessment and reporting procedures
- Interpret the DSS appropriately for merchants' specific environments
- Maintain up-to-date knowledge of PCI SSC standards and industry trends
- Report all opinions as factual, documented and defensible

The PCI SSC plans a phased implementation of the program through the end of 2009.

### Analysis

The introduction of the PCI DSS has driven badly needed improvements in merchants' and other card-accepting enterprises' handling of customers' card data, but the compliance process is plagued by inconsistencies and conflicts of interest. The planned quality assurance program will help with the inconsistency issue, but will do nothing to address the more important conflict-of-interest problem. QSAs continue to sell remediation and managed security services, and this practice casts doubts on the integrity of their assessments.

Card-accepting enterprises often complain that a QSA's interpretation of requirements will change between assessments, even when the controls do not. These changes may be justified, but QSAs frequently do not adequately explain the rationale for the changes, their ultimate determinations or the remedial measures they prescribe. Assessors and audited enterprises often disagree about what parts of the enterprise's network are within the audit's scope, and assessments also depend heavily on the individuals performing them, which makes them essentially nonrepeatable. Moreover, QSAs' reporting requirements for demonstrating ongoing compliance typically are poorly defined and differ across periodic assessments.

The new program may help to mitigate these problems, if the SSC provides adequate staff to proactively monitor and improve the quality of assessments. But the most significant enterprise complaint about PCI compliance practices is that many assessors also offer products and services that can be used to meet DSS requirements and ensure compliance to the audit. The PCI takes the same self-regulating approach to this issue that is widely regarded as having failed in the financial auditing industry and having led to the separation of consulting and accounting audit services. Gartner believes that the only truly effective approach is for the PCI to prohibit QSAs from performing remediation services for enterprises they are assessing.

## RECOMMENDATIONS

---

### Merchants and other card-accepting enterprises:

- Continue to focus on end-to-end encryption or, wherever possible, reducing or eliminating the storage of card data, to reduce the scope of PCI liability

- If QSAs try to sell other products of services, or provide poor support, notify the SSC and your sponsoring bank, via e-mail to [qsa@pcisecuritystandards.org](mailto:qsa@pcisecuritystandards.org) or using the online form at [https://www.pcisecuritystandards.org/docs/gsa\\_feedback\\_form\\_-\\_client.doc](https://www.pcisecuritystandards.org/docs/gsa_feedback_form_-_client.doc). Notify your sponsoring bank as well.

## RECOMMENDED READING

---

- "Visa Sets Global PCI Deadlines, but Other Players Needed" — Visa's new global PCI DSS compliance program leaves many issues outstanding, including unclear European deadlines and the treatment of merchants that have chip card processing in place. **By Avivah Litan**
- "PCI Security Standard Update Does Not Meet Merchants' Needs" — The first update to the PCI DSS in more than two years does not address merchants' most critical security and compliance issues. **By Avivah Litan and John Pescatore**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## REGIONAL HEADQUARTERS

---

### Corporate Headquarters

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### European Headquarters

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### Japan Headquarters

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### Latin America Headquarters

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509