

# Re: Importance of being a QSA

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-11/msg00193.html>

---

- *From:* "Kurt Grutzmacher" <[grutz@xxxxxxxxxxxxxx](mailto:grutz@xxxxxxxxxxxxxx)>
  - *Date:* Tue, 28 Nov 2006 10:13:07 -0800
- 

On 11/28/06, 3 shool <[3shool@xxxxxxxxxx](mailto:3shool@xxxxxxxxxx)> wrote:

Hi All,

We have been doing Penetration tests for more than 4 years for our customers, including financial and e-commerce segments. One of our customer came up with a requirement that they would get PenTest services ONLY from QSA (Qualified Security Assessor) by PCI, as part of company policy.

We have been delivering fantastic results for them over the years and they too haven't had any security breaches during this period. I have heard about this in the mailing list last year but just wanted to know how important it is to be a QSA for companies like us who have been doing PenTests since a good period.

Is it just a marketing strategy or is it something more than OSSTMM or other methodologies that we don't account for in our tests?

Welcome to the 21st Century for Penetration Testing. If you're going to want/need certification from PCI then you have to follow what PCI says. Our industry has been pretty wild west for some time and it's now being wrangled to fit into auditor-like qualities. OSSTMM was a start, PCI's QSA is just the next evolution.

[https://www.pcisecuritystandards.org/certification/how\\_to\\_become\\_a\\_qsa.htm](https://www.pcisecuritystandards.org/certification/how_to_become_a_qsa.htm)

It kind of makes me feel like we're becoming sad Elevator Inspectors (no disrespect to elevator inspectors, I'm sure they're really happy people). Just another check-off to make people feel safer about putting in their credit card information.

So pay your PCI fee, your (ISC)2 fee, your OWASP donation, your ISECOM certification, get your insurance together and continue to do your work. If the customer demands it there usually is a reason. In this case my guess is because they want to be PCI certified.

---

Re: Importance of being a QSA

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

[http://www.cenzic.com/products\\_services/download\\_hailstorm.php?camp=70160000008bOW](http://www.cenzic.com/products_services/download_hailstorm.php?camp=70160000008bOW)

---