

RE: How does a customer get PCI audited?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-06/msg00099.html>

- *From:* Craig Wright <Craig.Wright@xxxxxxxxxx>
 - *Date:* Thu, 5 Jun 2008 13:17:46 +1000
-

Hi Erin,

I would disagree. I would split off "compliance" and "perception of compliance". Passing an audit is evidence that a system could be compliant. A compromise of a system using a known vulnerability is strong evidence that it is not compliant.

A system that is breached due to a complex password and secured key that was "guessed" is possible, though unlikely. This would be one of the few examples of a compliant system that is also breached. Basically, it will be rare to find a compliant system (to any jurisdiction) that is easily compromised.

What I learnt completing my LLM was how few systems are compliant. How little knowledge there is of the law and legal frameworks already in place (even with politicians) and the lack of due care. An ABSOLUTE baseline for a compliant system that has no other effect other than being owned by a company would be the CISecurity.org baselines at 100%.

The combination of technical people with no knowledge of the legal system, laws and processes with lawyers who can not turn on a PC is an issue here.

"I would agree with Adriel that finding a worthwhile auditor is difficult". Actually so would I. Finding a staff with half a brain provides enough difficulty to want to give up on the whole idea.

"The problems are analyzed from a primarily financial and business risk avoidance perspective"

Here I have to disagree. I work with financial auditors and I am yet to meet one who understands risk and have met very few who have the faintest comprehension of finance. Audit and finance are NOT the same thing. I did finance at a masters level and I think audit is wacky for the most part. For the rest, there is an approach of try to find nothing wrong or it will upset the client.

I have developed statistically based continuous audit programs for financial systems. These have a significantly lower cost and deliver more. What I get back is "Craig, we are watch dogs and not blood hounds. Please try not to find so much". So I use these with the Insolvency teams and on forensic audits, but it is a hard sell to audit teams. Clients seem to love it though..

"I'm curious as to what vulnerable points you're thinking of."