

# Geek Week 2010

## PCI Assessment – What Does it Really Mean?

**Reggie Letson CISSP, CISA**

**IT Compliance Architect**

**The Home Depot**

**“Disclaimer:**

**Views and opinions presented by Speaker during this presentation do not necessarily represent the views and opinions of current and former employers.”**

# PCI Assessment - What does it really mean?

**It Depends**

# How do I assess that I am PCI Compliant?

1. **What are you assessing as? Merchant or Service Provider?**
2. **What Merchant Level are you?**
3. **Do you have to have an onsite assessment performed?**
4. **Can you self assess?**
5. **What is the PCI Security Council?**

**The PCI Security Standards Council organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and VISA, Inc.**

**<https://www.pcisecuritystandards.org/index.shtml>**

# [http://usa.visa.com/merchants/risk\\_management/cisp\\_overview.html](http://usa.visa.com/merchants/risk_management/cisp_overview.html)

Level / Tier <sup>1</sup>	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region <sup>2</sup>	<ul style="list-style-type: none"><li>• Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”)</li><li>• Quarterly network scan by Approved Scan Vendor (“ASV”)</li><li>• Attestation of Compliance Form</li></ul>
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none"><li>• Annual Self-Assessment Questionnaire (“SAQ”)</li><li>• Quarterly network scan by ASV</li><li>• Attestation of Compliance Form</li></ul>
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none"><li>• Annual SAQ</li><li>• Quarterly network scan by ASV</li><li>• Attestation of Compliance Form</li></ul>
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none"><li>• Annual SAQ recommended</li><li>• Quarterly network scan by ASV if applicable</li><li>• Compliance validation requirements set by acquirer</li></ul>

## VISA - Compliance Stats

[http://usa.visa.com/download/merchants/cisp\\_pcidss\\_compliancestats.pdf](http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf)

# How Do I Maintain Compliance Year After Year?

1. Look for ways to reduce your scope for PCI?
2. Look for ways to improve your controls and/or processes.
3. Are there ways to automate some of the manual efforts?
4. Are there ways to combine synergies with other compliance efforts?

**“Disclaimer:**

**Views and opinions presented by Speaker during this presentation do not necessarily represent the views and opinions of current and former employers.”**

Questions?



## References:

Slide 5. PCI Security Standards Council website.

<https://www.pcisecuritystandards.org/index.shtml>

Slide 6. VISA website

[http://usa.visa.com/merchants/risk\\_management/cisp\\_overview.html](http://usa.visa.com/merchants/risk_management/cisp_overview.html)

Slide 7. VISA website

[http://usa.visa.com/download/merchants/cisp\\_pcidss\\_compliancestats.pdf](http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf)