

# PCI Compliance

Live Long and Prosper

Presented by

**Andrew Plato, CISSP, CISM, QSA**

President / Principal Consultant

Anitian Enterprise Security

# Who am I?

**Andrew Plato, CISSP, CISM, QSA**

*President / Principal Consultant,  
Anitian Enterprise Security*

- **Owner, founder and chief executive for Anitian**
- **15 years experience in information security**
- **Previous jobs: programmer, DBA, tech writer**
- **Completed 1500+ security projects and 500+ assessments.**
- **Practical, pragmatic approach to security**

**COMPLIANCE & ASSESSMENT**

1

Penetration Testing, Code Review, PCI Compliance, Risk Assessment, Policy Development, Forensics

**SOLUTIONS & TECHNOLOGIES**

2

Firewalls, IPS, SSL-VPN, SIM/SEM, Endpoint Security, Encryption, Identity & Access Management

**MANAGEMENT & SUPPORT**

3

Managed Security, Analysis & Investigation Services, Staff Augmentation, Incident Response



# The Anitian Advantage

## Clear, Effective Vision for Information Security

- ✓ Practical, pragmatic approach to information security & compliance.
- ✓ Rational, realistic risk assessment techniques.

## Unmatched Experience

- ✓ Oldest security firm in the nation.
- ✓ Proven success with 2000+ customers.
- ✓ Full spectrum of security experience.

## Thought Leadership

- ✓ Smart people who can solve tough problems.
- ✓ Business-oriented, without the “hacker” attitude.
- ✓ Visionary guidance and recommendations.

# Overview

- ❖ **PCI Myths and Misunderstandings**
- ❖ **12 Building Blocks of PCI Compliance**
- ❖ **How to Prioritize Your Compliance Efforts**

# Defining Moment

- ❖ PCI DSS
- ❖ Qualified Security Assessor (QSA)
- ❖ Payment Brands (Visa, MC, Amex, Discover, JCB)
- ❖ Merchant
- ❖ Third Party Provider (TPP)
- ❖ Acquirer
- ❖ Bank
- ❖ Processor
- ❖ Primary Account Number (PAN)
- ❖ Cardholder Data Environment (CDE)

# PCI Merchant & TPP Levels

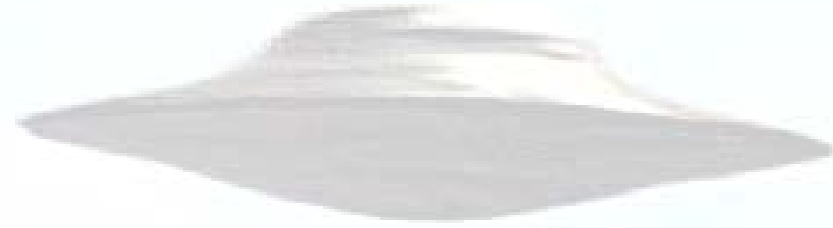
- ❖ Each payment brand has their own levels for merchants and TPPs
- ❖ Visa's levels tend to trump all the others.

Level	Merchants	TPPs
1	More than 6M transactions (any method) or any merchant that has had a breach or any merchant Visa decides is a Level 1.	Any TPP that stores, processes and/or transmits more than 300,000 transactions (any method)
2	1M – 6M transactions per year, any method.	Any TPP that stores, transmits and/or processes less than 300,000 transactions (any method)
3	Less than 1M transactions of which more than 20,000 of those are e-commerce transactions	N/A
4	Less than 1M transactions and no more than 20,000 e-commerce transactions.	N/A

# Validation & Reporting

- ❖ Each brand has their own validation & reporting requirements – for merchants and service providers
- ❖ Visa’s merchant requirements tend to lead the pack here as well:

Level	Validation	Reporting
1	<ul style="list-style-type: none"><li>• Annual on-site QSA assessment</li><li>• Quarterly ASV scans</li></ul>	<ul style="list-style-type: none"><li>• Report on Compliance and/or</li><li>• Attestation of Compliance</li></ul>
2	<ul style="list-style-type: none"><li>• Annual self-assessment</li><li>• Quarterly ASV scans</li></ul>	<ul style="list-style-type: none"><li>• Annual self-assessment questionnaire</li><li>• Attestation of Compliance</li></ul>
3	<ul style="list-style-type: none"><li>• Annual self-assessment</li><li>• Quarterly ASV scans</li></ul>	<ul style="list-style-type: none"><li>• Annual self-assessment questionnaire</li></ul>
4	<ul style="list-style-type: none"><li>• Annual self-assessment</li><li>• Quarterly ASV scans</li></ul>	<ul style="list-style-type: none"><li>• Annual self-assessment questionnaire</li></ul>



# PCI Compliance Myths & Misunderstandings

**MYTH**      *We outsource our processing, therefore PCI compliance does not apply to our business.*

**TRUTH**      Compliance is required if you...

- *Transmit ANY payment card data across any part of your network...OR*
- *Store any sensitive payment card data anywhere in any format....OR*
- *Process payment cards internally.*

**Outsourcing can reduce PCI requirements that apply to your organization, but not completely eliminate them.**

**MYTH** *Our bank or payment processor does not require us to be PCI compliant.*

**TRUTH** They probably have not gotten to you, yet.  
Banks (acquirers) are ultimately responsible for the compliance of their merchants.  
Ignoring PCI compliance shows a disregard for risk management - which is not something you want in a financial institution (especially considering current events.)

**MYTH**      *We ran a scan, so we're compliant.*

**TRUTH**      **Scanning is only one aspect of compliance.  
External scans must be conducted by an  
Approved Scanning Vendor to be legitimate.  
Penetration testing and internal scanning are  
also required.**

**MYTH** *We are too small for PCI compliance. Our sales amounts are too small.*

**TRUTH** PCI applies to all organizations, of any size.  
Low transaction counts only reduce your reporting and validation requirements.  
It does not exclude you from compliance.  
The dollar amount of transactions is irrelevant to PCI compliance.

## MYTH

*It is impossible to be compliant. It is too complicated and too expensive.*

## TRUTH

The requirements are best practices you should already be following.

More than 85% of the large, level 1 merchants are compliant.

If there is breach, then whatever you spend on compliance will pale in comparison to the clean up and legal costs.

There are numerous inexpensive ways to become compliant.

**MYTH**      *We purchased a “Compliance Appliance” that handles everything and makes us compliant.*

**TRUTH**      **There is no such thing as a single application or appliance that can make you compliant.**

**Be very wary of any company selling an “all in one” compliance solution.**

**Compliance is a process, technologies are only part of the process.**

*NOTE: The PA-DSS does certify applications, but it is for COTS software providers.*

**MYTH**      *PCI compliance is an IT project.*

**TRUTH**      **PCI is a business risk issue.**

**A PCI compliance effort requires a multi-disciplinary team that involves many parts of the organization including: finance, operations, management, human resources – as well as IT.**

**IT is a big part of the technical aspects of compliance.**

**Management buy-in is critical.**

**MYTH** *PCI is only for e-commerce transactions.  
We do everything manually.*

**TRUTH** PCI applies to any organization that stores, transmits or processes payment cards.  
The lack of e-commerce does not exclude you from compliance.  
PCI also covers physical records, such as receipts.

**MYTH** *Nobody gets fined, we will just accept the risk or buy insurance.*

**TRUTH** Nobody is going to tell you they got fined.  
Fines are very real.  
Liability is the more serious problem.  
If you have a breach, the lawsuits will overwhelm you.  
Ignoring compliance is a negligent business practice.  
Insurance companies are not going to cover this risk.

# PCI Compliance Is Not That Difficult

- ❖ All of the requirements are good practices you should already be doing.
- ❖ The standard is meant to be interpreted.
- ❖ Once compliant, maintenance is fairly easy.
- ❖ A good PCI compliance effort should empower your business, not hinder it.
- ❖ Smaller organizations can self-certify.



*There has to be a better way.*

# The PCI DSS Standard

1. **Install & maintain a firewall**
2. **Do not use vendor defaults**
3. **Protect card holder data**
4. **Encrypt transmission of cardholder data across public networks**
5. **Use & update anti-virus**
6. **Develop and maintain secure applications**
7. **Restrict access to cardholder data to least privilege**
8. **Assign a unique ID to all users**
9. **Restrict physical access to cardholder data**
10. **Track and monitor all access**
11. **Regularly test systems and processes**
12. **Maintain a security policy the addresses information security**



# PCI Compliance Building Blocks



# 1. Segregate & Isolate Payment Systems

- ❖ Compliance requirements can be limited to only those systems that handle payment card data – provided it is segregated and isolated.
- ❖ Define the cardholder data environment.
- ❖ Isolate it with:
  - Firewalls
  - VLANs & ACLs
  - Physical separation



*We are the Cisco. We will add your VLANs and ACLs to our configuration. Your network will service us. Resistance is futile.*

## 2. Log Management / SIM

- ❖ PCI requires daily review of event logs
- ❖ Realistically this means some type of automated log analysis
- ❖ Security Information (or Event) Management (SIM) solutions are an ideal choice, since they provide more than just log management
- ❖ Evaluate solutions carefully, not all SIMs are alike



### 3. Two Factor Authentication

- ❖ Simple answer to a variety of risks.
- ❖ A must for remote access into the CDE.
- ❖ Has become inexpensive and easy to implement.
- ❖ Makes hacking significantly more difficult.
- ❖ Improves auditing.
- ❖ Two factor is not the same as two logins.



## 4. Host Data Protection

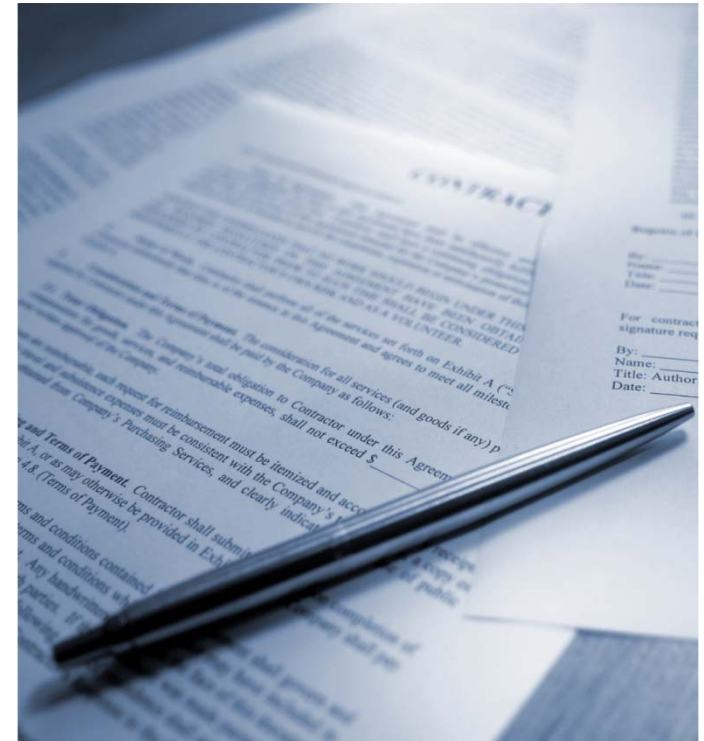
- ❖ **Must Haves (for in-scope hosts):**
  - **Antivirus**
  - **Integrity monitoring**
  - **Log monitoring**
  - **Patch management**
  - **Vulnerability scanning**
  - **Policies that define how these are used, managed, etc.**
  
- ❖ **Good to Haves:**
  - **Host IPS**
  - **Data loss prevention**
  - **Whole disk encryption**



*Sensitive data, its everywhere you don't want it to be.*

## 5. Align Policies With PCI

- ❖ Your organizational policies should specifically identify the 12 PCI requirements.
- ❖ Policies should map to each requirement.
- ❖ Make this clear and easy for an auditor to find.
- ❖ This is the most difficult aspect of PCI compliance.
- ❖ Invest in a good writer.





## 7. Manage Change

- ❖ Undocumented change represents a huge risk to your organization
- ❖ Change management is not sexy or interesting – but vital
- ❖ Consider managed security providers
- ❖ Stand up to management's whims, make them justify changes
- ❖ Get your contractors on your ticketing system
- ❖ Manage application vendors



*Eh, nobody will notice when I install this chat program on the mail server.*

## 8. Firewalls & IPS

- ❖ You must have both, period.
- ❖ Document management processes.
- ❖ Unified Threat Management (UTM) solutions are a great way to save money.
- ❖ Be careful with managed solutions, not all are equal.
- ❖ Good IPS's can provide a very valuable “gap protection” when new exploits are released.



*Pew pew pew pew!*

## 9. Encrypt It All

- ❖ Inside the cardholder data environment...
  - Encrypt the network traffic.
  - Encrypt the data.
  - Encrypt the wireless (WPA2).
  - Encrypt the database.
  - Should we...yes, encrypt that too.
- ❖ Encryption is not security.
- ❖ Manage the keys or forget it.



# 10. Conduct Regular Security Assessments

- ❖ A \$50 scan isn't going to cut it
- ❖ You must perform the following:
  - External ASV scan of all active hosts quarterly.
  - Annual network penetration test (internal & external.)
  - Annual web application test on all externally exposed web apps.
  - Annual risk assessment.
  - Regular internal vulnerability assessments.



# 11. Vendors Must Be Compliant Too

- ❖ Any third party vendors you work with who handle cardholder data must also be compliant. Such as:
  - Hosting providers
  - Off-site storage & backups
  - Credit card processors
  - Application vendors
- ❖ You need contractual proof of their compliance or they must agree to take FULL responsibility for any breach.



*Oh suuuure, we're compliant. We're huge. Massive. All the big-boys use us. Yep, just sign here.*

## 12. Who's the Boss?

- ❖ For merchants, you owe compliance your acquirer.
- ❖ For service providers, customers will demand PCI compliance.
- ❖ You need to understand your compliance environment.
- ❖ Merchants – talk with your acquirer and find out what they expect.
- ❖ Service Providers – talk to customers, find out what they need.



## Remember...

- ❖ **Technology is only part of the problem.**
- ❖ **Don't store payment card data, if you don't have to.**
- ❖ **Don't let sales people drive your compliance efforts.**
- ❖ **Only a QSA can certify PCI compliance or sign-off on a self-assessment.**
- ❖ **Compliance is not security, but PCI is a good foundation.**
- ❖ **It is not that difficult!**



*Say you like the beard! Say it!!!*

# **Prioritize Your Compliance Efforts**

**The ultimate goal of PCI is to protect cardholder data & its associated environment(s)**

## **FIRST – Secure The Environment**

**Upgrade your infrastructure and technologies to provide active protections against a breach.**

## **SECOND – Implement Sound Practices**

**Improve management and monitoring of your environment.**

## **THIRD – Document Effective Policies**

**Write and disseminate good policies, procedures and standards**

# How Can Anitian Help?

- ❖ **PCI Gap Assessment**
- ❖ **PCI Compliance Audit with ROC/AOC**
- ❖ **Penetration Testing & Web Application Testing**
- ❖ **Quarterly ASV Scans with Compliance Portal**
- ❖ **Remediation technologies and solutions**
- ❖ **PCI Policy development**
- ❖ **PCI Compliance Suite**
  - **Gap Assessment**
  - **PCI Audit**
  - **Penetration Testing**
  - **Internal & external vulnerability scanning**

# Thank You

You can get a copy of this presentation off  
the Anitian web site at:

[http://www.anitian.com/white\\_papers.html](http://www.anitian.com/white_papers.html)

## My Contact information:

Andrew Plato, CISSP, CISM, QSA  
President / Principal Consultant  
Anitian Enterprise Security  
andrew.plato@anitian.com  
888-ANITIAN