The Payment Card Industry's laws and contractual compliance obligations

What you need to know about the Payment Card Industry's various compliance contractual obligations, standards, and surrounding laws

Your instructor

Steven M. Helwig, CISSP

Title: Director of Professional Services and Policy Analyst

Company: Compliance Spectrum / Unified Compliance Framework

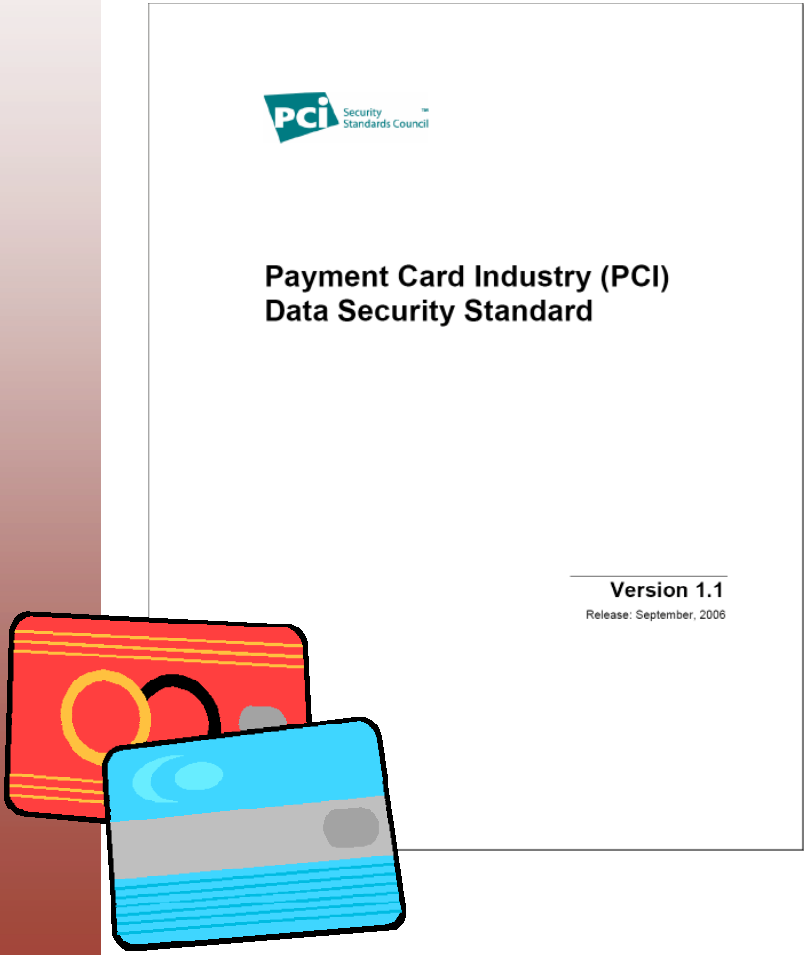
Contact: steve.helwig@compliancespectrum.com
512 – 535 - 7794

Education: MSIS, MBA

Publications: Technical Editor on Policy Writing Book, Member of PCI SSC

Course objectives

By completing this course, you will learn about:



PCi Security Standards Council™

Payment Card Industry (PCI)
Data Security Standard

Version 1.1

Release: September, 2006

- **The PCI-DSS standard** and how it fits within a commerce-focused Unified Compliance Framework
- **Building and maintaining a secure network**
- **Protecting cardholder data**
- **Creating and maintaining a vulnerability management program**
- **Implementing strong access control measures**
- **Monitoring and maintaining the networks**
- **Maintaining an information security policy**

The PCI-DSS standard

And how it fits within a commerce-focused
Unified Compliance Framework

The PCI-DSS standard overview

Where does the PCI-DSS fit in the world of compliance?

- Some basics about the Payment Card Industry’s Security Standards Council and their Data Security Standard
- IS PCI-DSS a regulation or a standard?
- Where does PCI-DSS fit within the world of unified compliance?

The PCI-DSS and the PCI-SSC

- The PCI Security Standards Council was launched on September 7th, 2006
- The *founding brands* that are a part of the PCI Security Standards Council (PCI SSC) are
  - JCB and Visa International
  - American Express
  - Discover Financial Services
  - MasterCard Worldwide
- The PCI SSC now extends to key 3rd parties

- PCI SSC Scope
  - Develop and manage the PCI-DSS
  - Manage the approval process for assessors and scanning vendors
  - Develop and publish PCI-DSS related documents
- PCI SSC *not in scope*
  - Compliance tracking and enforcement
  - Forensics and Account Data Compromise (ADC) event response

http://www.pcisecuritystandards.org

PCI-DSS: a regulation or a standard?

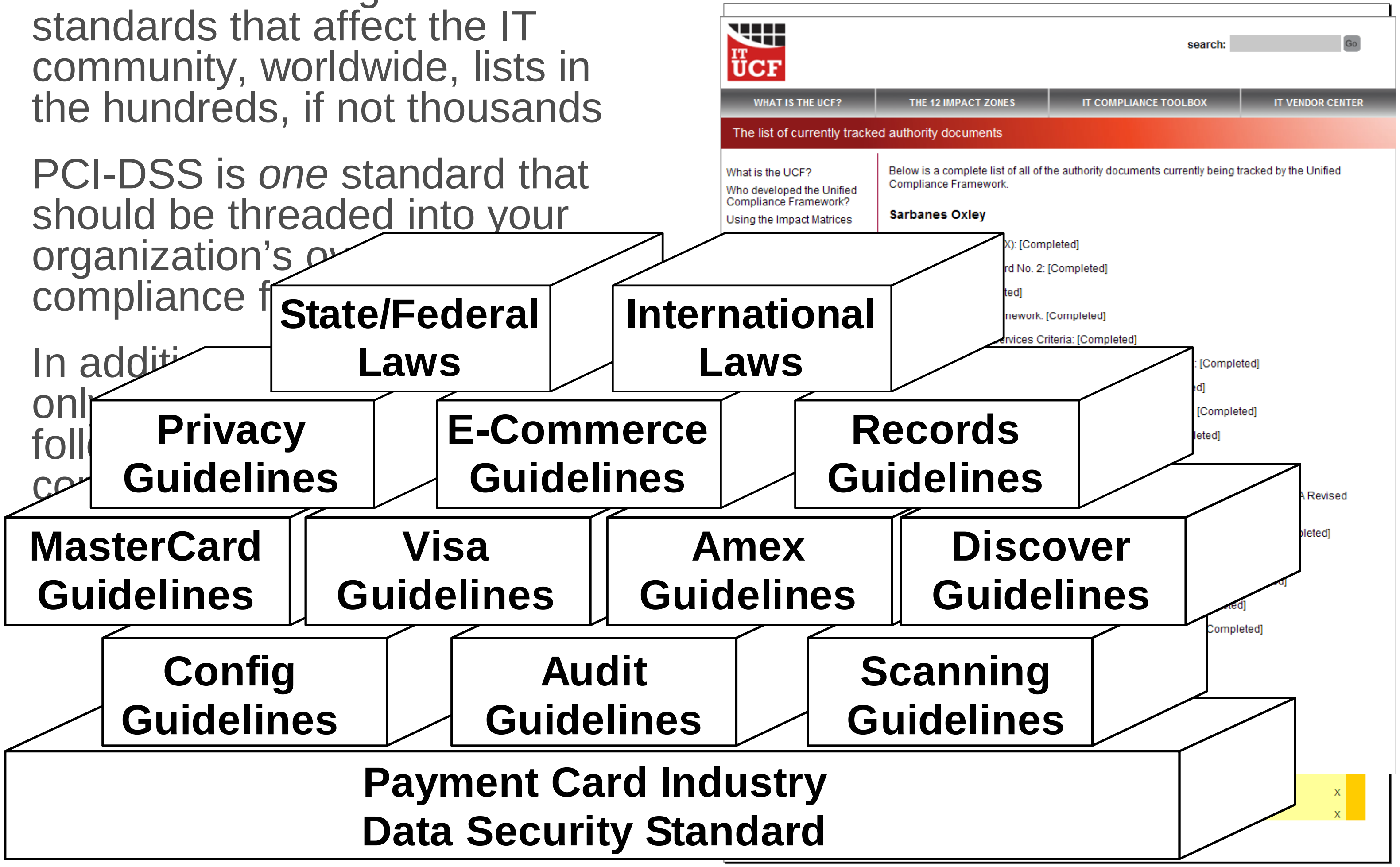
- Regulation
  - To regulate is to bring under *the force of law* or a *governing authority*.
  - The regulators are empowered to interpret how the laws are to be implemented and to establish rules for following those laws. Those rules are then documented as **regulations**.

- Standards
  - *Standards are not enforceable by law*. *However, failure to follow standards may result in actions contrary to regulations which* ***are*** *enforceable by law*.
  - A standard is a criterion, a means of determining what rules, principles, and measures established by an authority should apply to a given situation in order to improve efficiency.

- PCI-DSS is a *hybrid*
- The Payment Card Industry Association also mandates the use of its PCI-DSS standard as the audit standard that must be followed when proving that you've met their guidelines.
  - Anyone wanting to accept credit cards as a form of payment is required to contractually agree to comply with this standard and failure to comply can result in a variety of fines and, potentially, the loss of the right to accept credit cards at all.

PCI-DSS in compliance overall

- The total list of regulations and standards that affect the IT community, worldwide, lists in the hundreds, if not thousands
- PCI-DSS is *one* standard that should be threaded into your organization's o compliance f
- In additi onl foll co



search: Go

WHAT IS THE UCF? | THE 12 IMPACT ZONES | IT COMPLIANCE TOOLBOX | IT VENDOR CENTER

The list of currently tracked authority documents

What is the UCF?

Who developed the Unified Compliance Framework?

Using the Impact Matrices

Below is a complete list of all of the authority documents currently being tracked by the Unified Compliance Framework.

Sarbanes Oxley

X): [Completed]

rd No. 2: [Completed]

ted]

nework. [Completed]

ervices Criteria: [Completed]

: [Completed]

d]

[Completed]

leted]

A Revised

pleted]

ted]

Completed]

State/Federal Laws

International Laws

Privacy Guidelines

E-Commerce Guidelines

Records Guidelines

MasterCard Guidelines

Visa Guidelines

Amex Guidelines

Discover Guidelines

Config Guidelines

Audit Guidelines

Scanning Guidelines

Payment Card Industry Data Security Standard

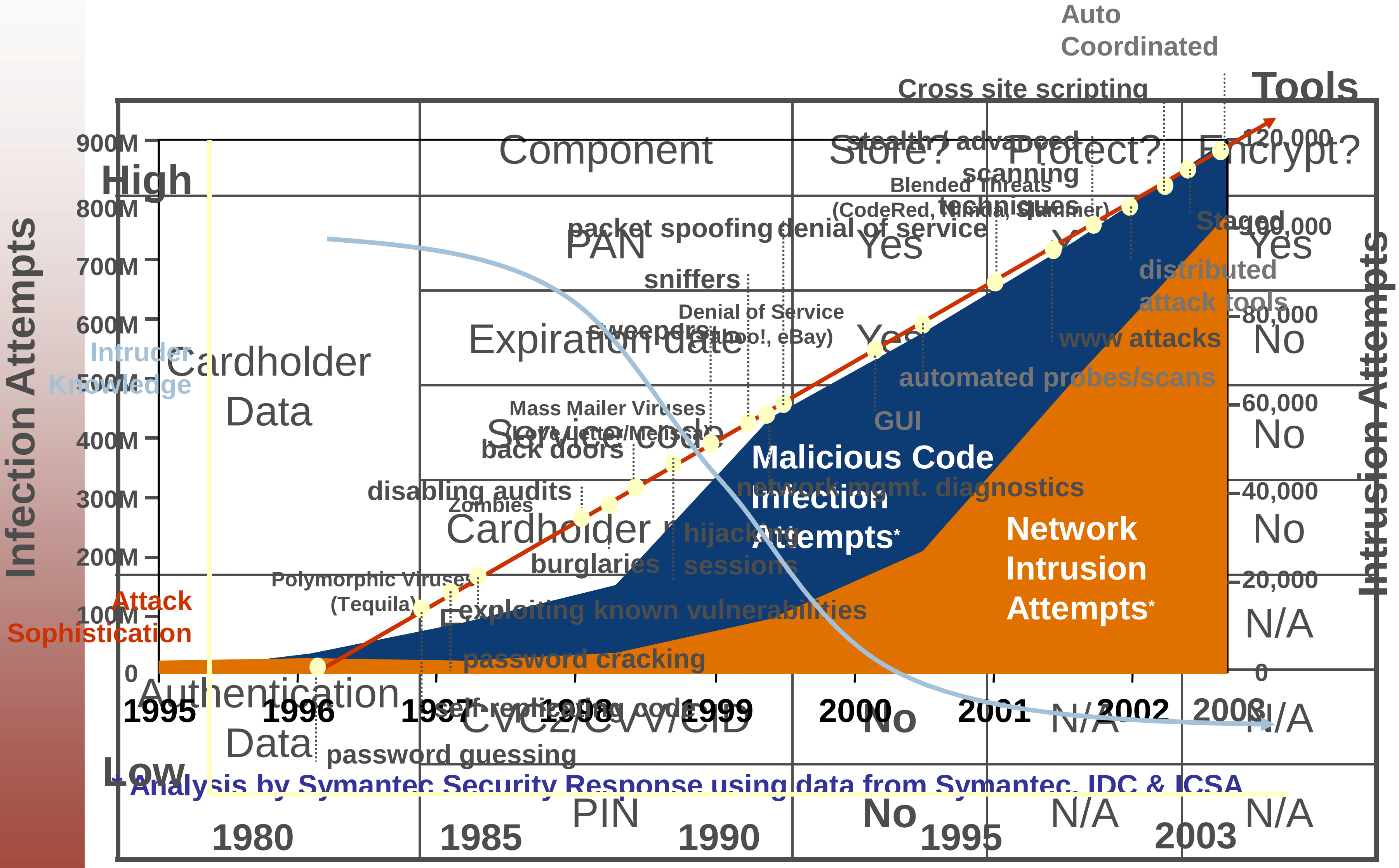
What are the threats?

The threats are legion

They are technical, physical, and people based

What does PCI-DSS seek to protect?

	Component	Store?	Protect?	Encrypt?
Cardholder Data	PAN	Yes		Yes
	Expiration date	Yes		No
	Service code			No
	Cardholder			No
Authentication Data	F			N/A
	CVC2/CVV2/CID	No	N/A	N/A
	PIN	No	N/A	N/A



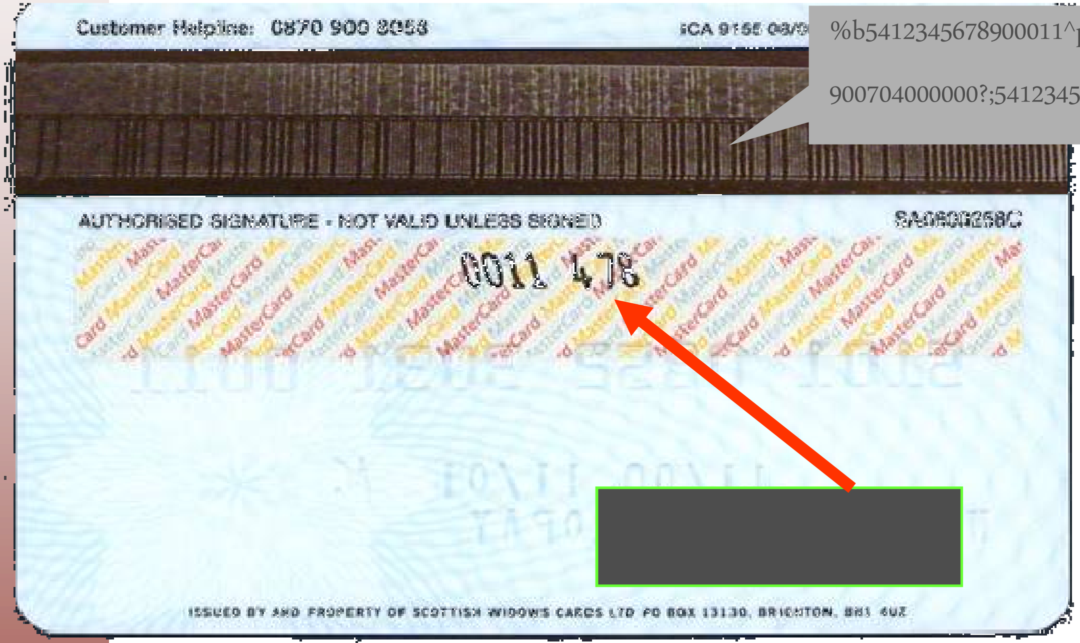
*Analysis by Symantec Security Response using data from Symantec, IDC & ICSA

New Payment Technologies

- New payment methods
  - Chip and PIN
  - Contactless
  - Mobile
- New terminals
  - IP enabled
  - Mobile

Same Threat

Most criminal organizations want to obtain:


Customer Helpline: 0870 900 8058
AUTHORISED SIGNATURE - NOT VALID UNLESS SIGNED
0011 478
ISSUED BY AND PROPERTY OF SCOTTISH WIDOWS CARDS LTD PO BOX 13130, BRIGHTON, BN1 4UZ

%b5412345678900011^peter chan^990610176130121

900704000000?;5412345678900011=9906101761301

Magnetic track data:

- PAN
- User name
- Expiry date
- CVC1

- And especially the PIN:

4 6 2 7

Why do criminals want this information?

- With the equivalent track 2 data the criminals can make magnetic stripe cards – lots of magnetic stripe cards
  - These can be used to perform Cardholder not present fraud

With the PIN

The criminals can use the cards to withdraw cash

at an ATM

Global fraud trend (2006 vs. 2005)

• Counterfeit	+21%
• Card Not Present	+52%
• Lost & Stolen	+12%
• All Fraud	+23%

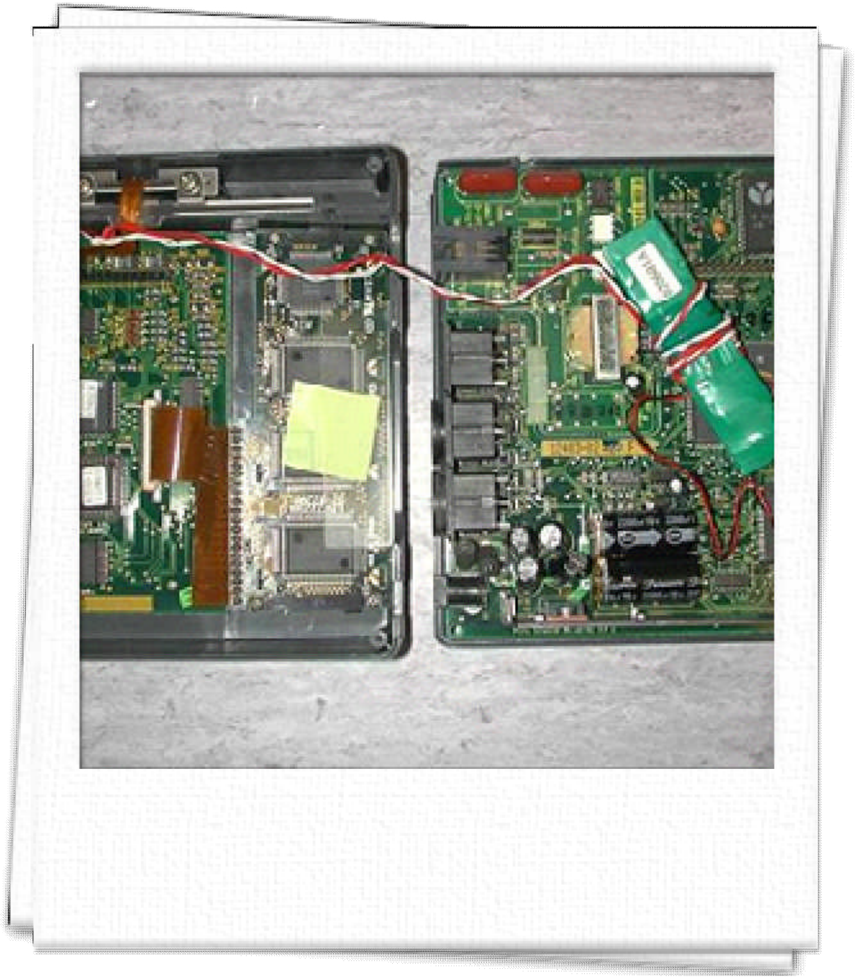
These figures hide significant regional variations, but cannot hide that Fraud remains a massive problem

What Is skimming?

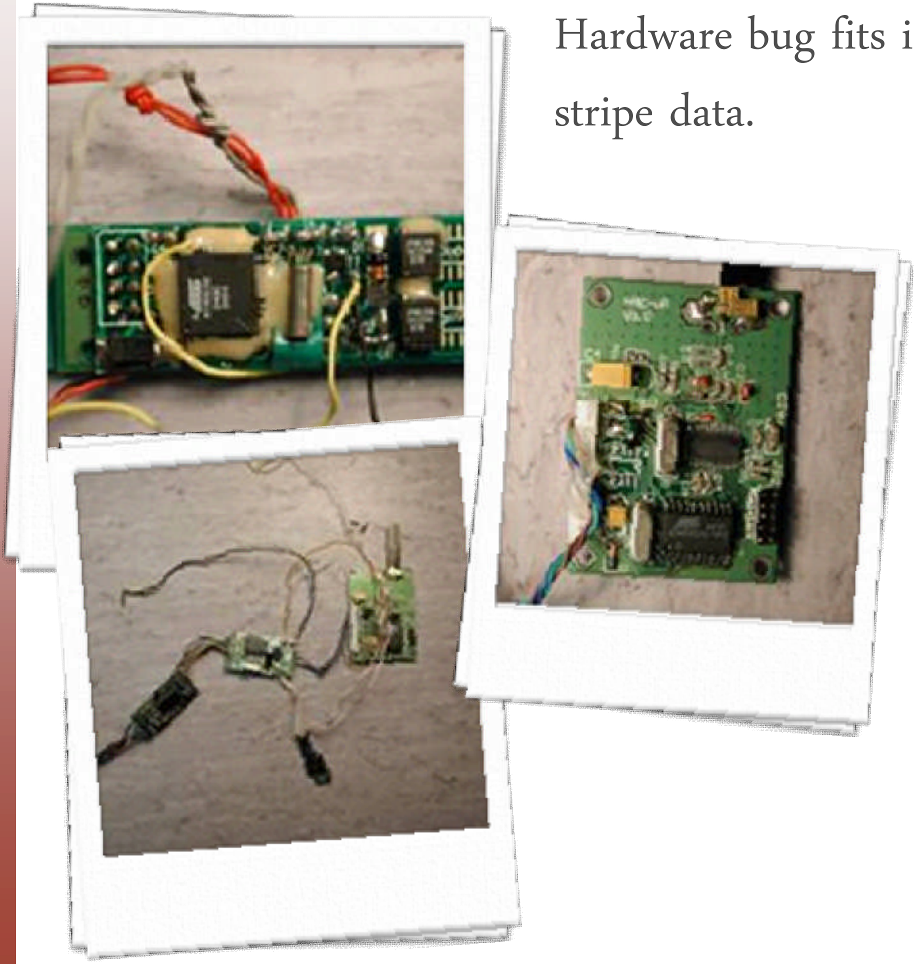
“Replication of electro … y or enable valid a

Where a PIN is not required magnetic stripe readers do not have to meet any security requirements and are therefore open to fraud

Implant a Skimmer into a terminal



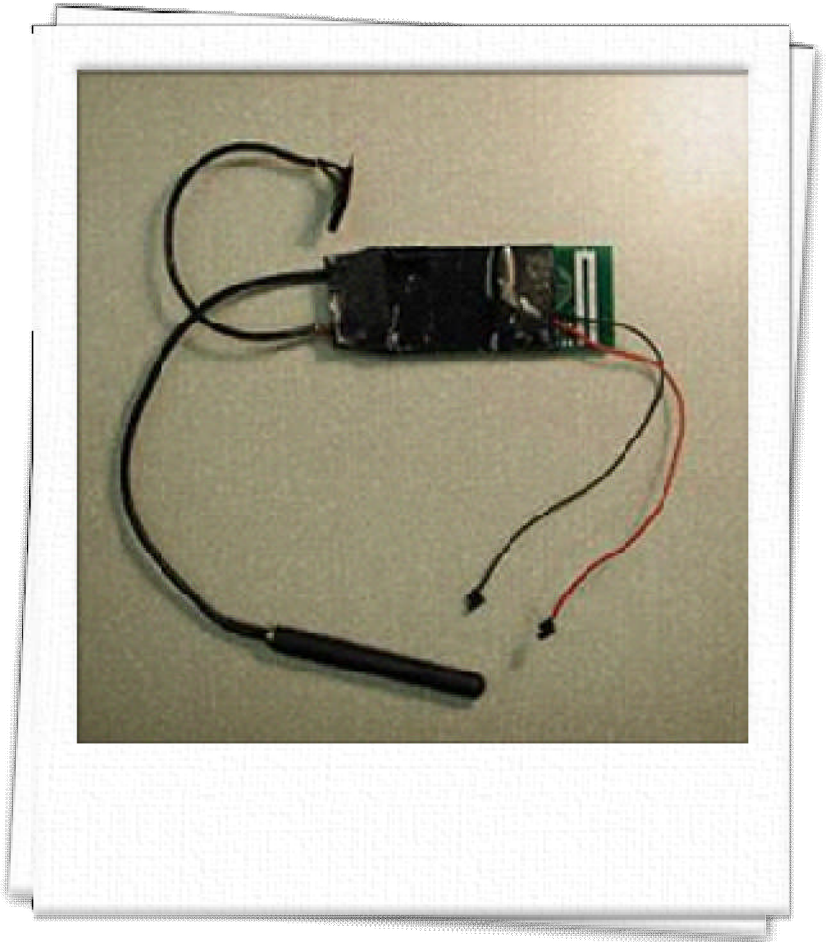
Skimmers are becoming more sophisticated

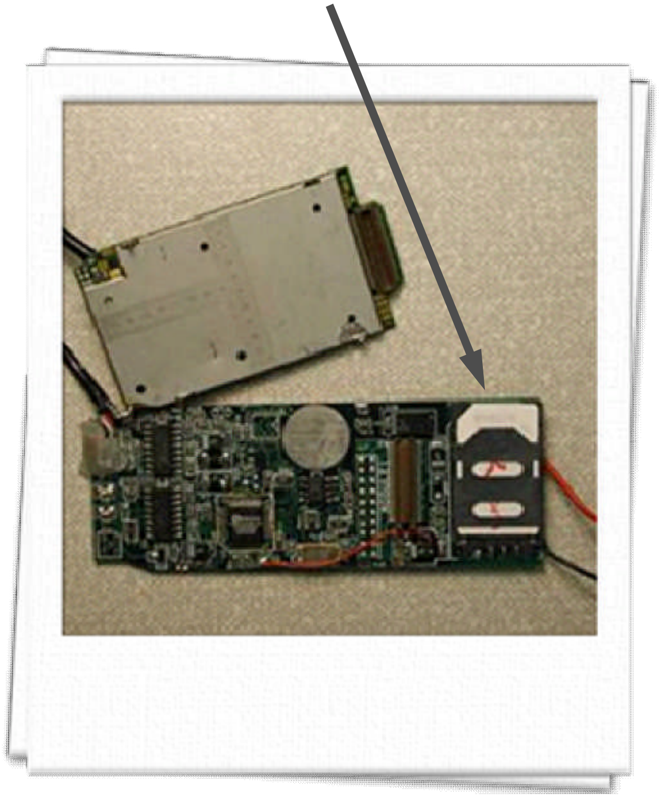


Hardware bug fits into a PED for tapping magnetic stripe data.

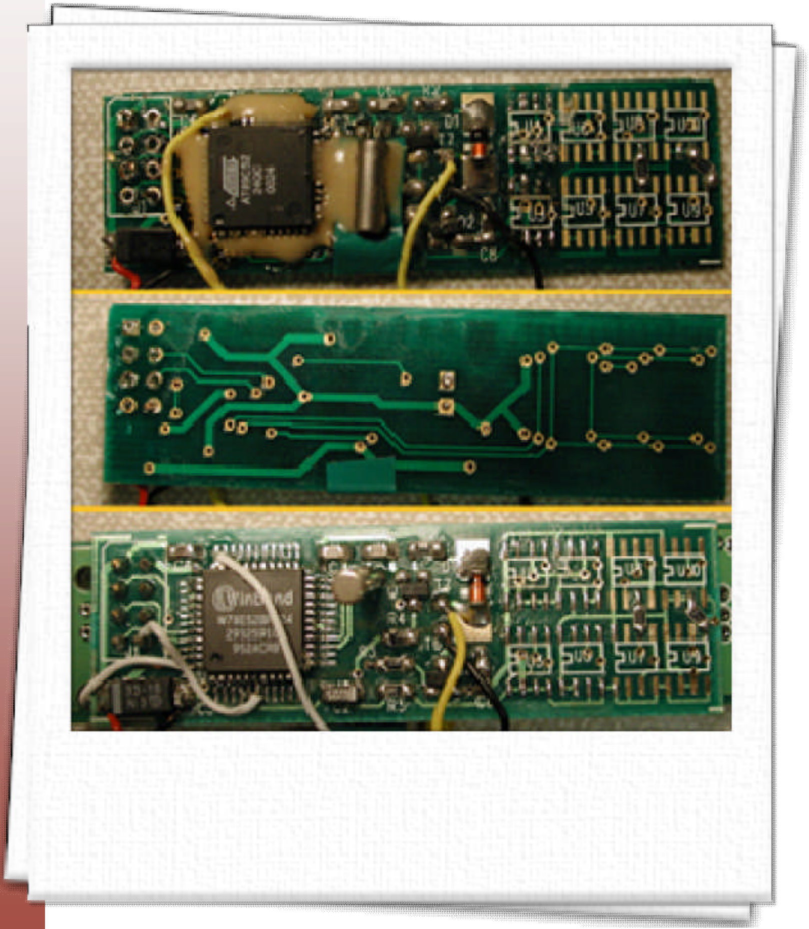
Transmitter, 200m range. Fits inside a PED.

GSM-based skimmers





Encoded memories



Encoded Data

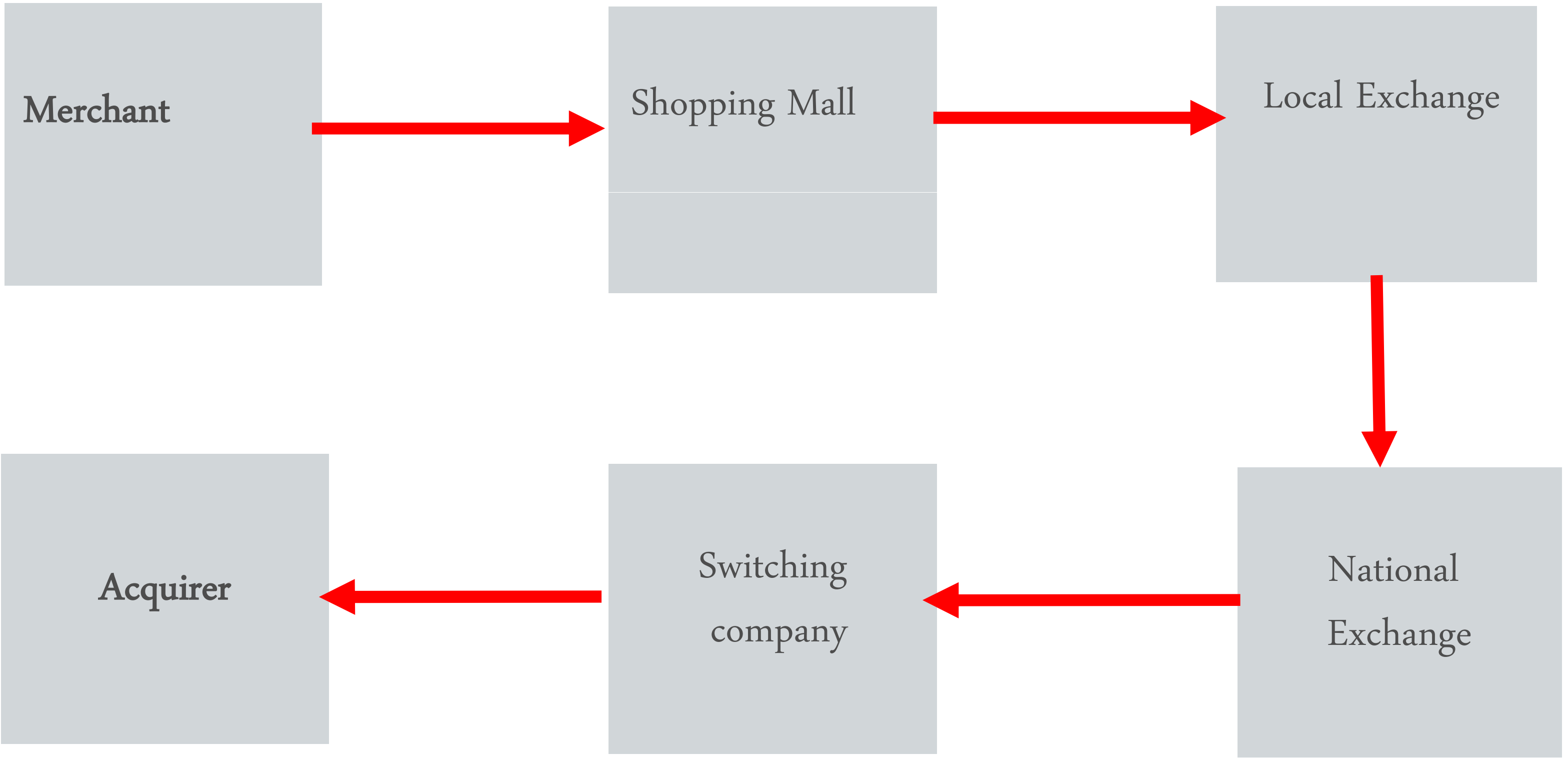
5DE308A72A419DF9005A9B8FE0EEF726A74EFC3DA6BEAD8A326FE1D7AD81E47539ED74BF32568EED17
4A8B9F8CEDF92EA24C925ECFCFCFF35811A0CCDAF092624B950AAF22469CFA00539C8DEFEDF92EA24
D905ECFCFCFF358189DC2DDFE9964419E30BA50439AFC0053938DE2EBF02DA04B905ECFA1B2812E6D8
DBAAE9BFE102A8169DA41228EFA004A8B9FF2F9E03FCE4C975ECDCECFF2581E9DC7DFE88A7558811D
BF32568EF23A519E8BE3EEF927A24C905ECDCFC8F1581E90C7DAF8986448900DAF22469EF23A4FE98AE6
E8F726A84E925CCFCDCFF45A1E9DA9A28AEC1658EC7CCC4633FCED632FF8EBF2EEF73FB05C824EDF
DFA1F35D1E9FC6DFF99A6548910DBF32568EED174A8B9FF2E6CD24A5489359C6C7CDF35A1E9FC7D8

Decoded Data

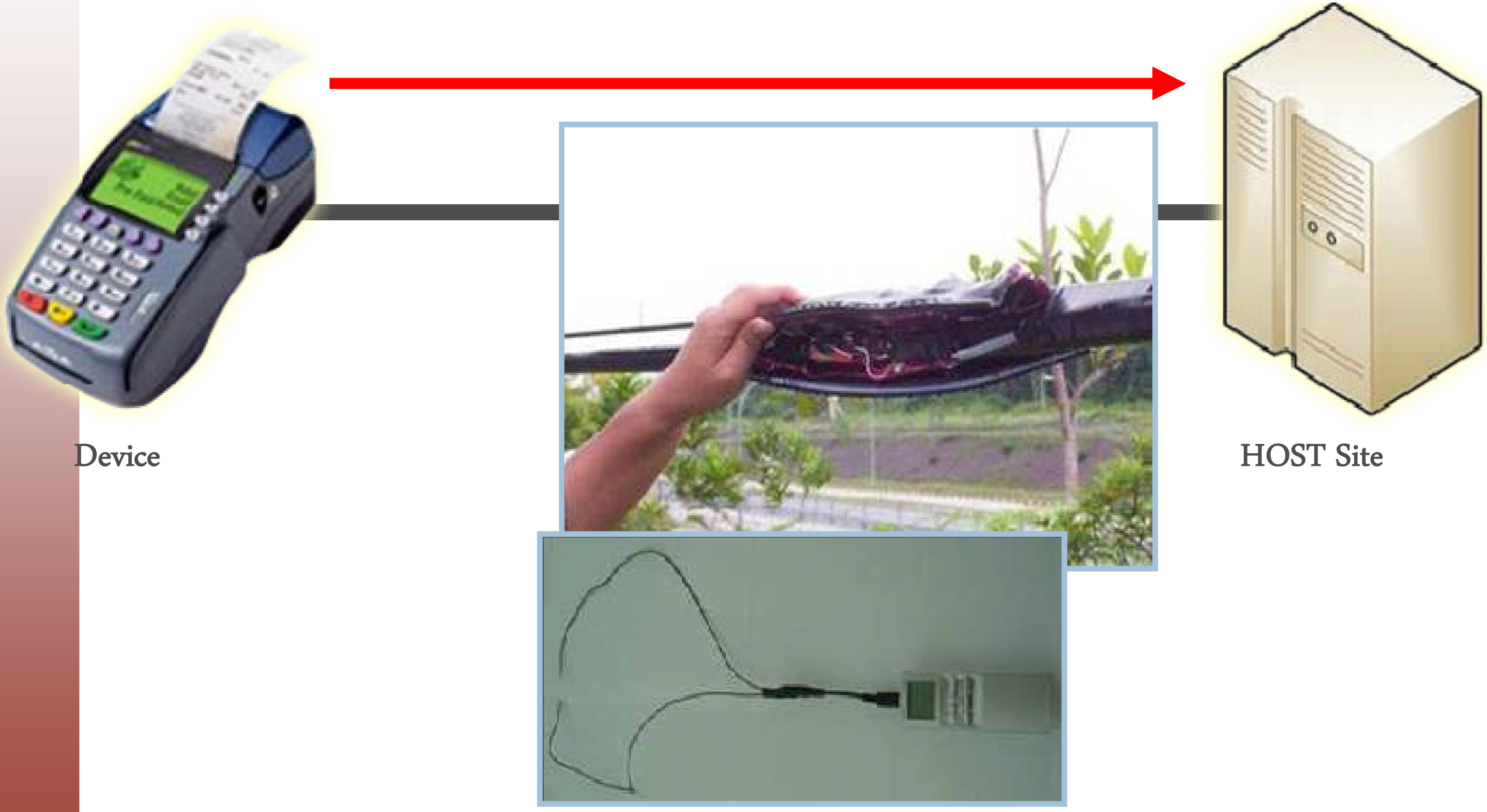
%B5567590310093267^A
^100510150000000000000103000000?
;5567590310093267=100510150000103?
%B5567590310093267^A
^100510150000000000000103000000?
;5567590310093267=100510150000103?
%B5567590310093267^A
^100510150000000000000103000000?

Wire tapping

- Wire tapping can occur at any point in the communication chain between Merchant and Acquirer

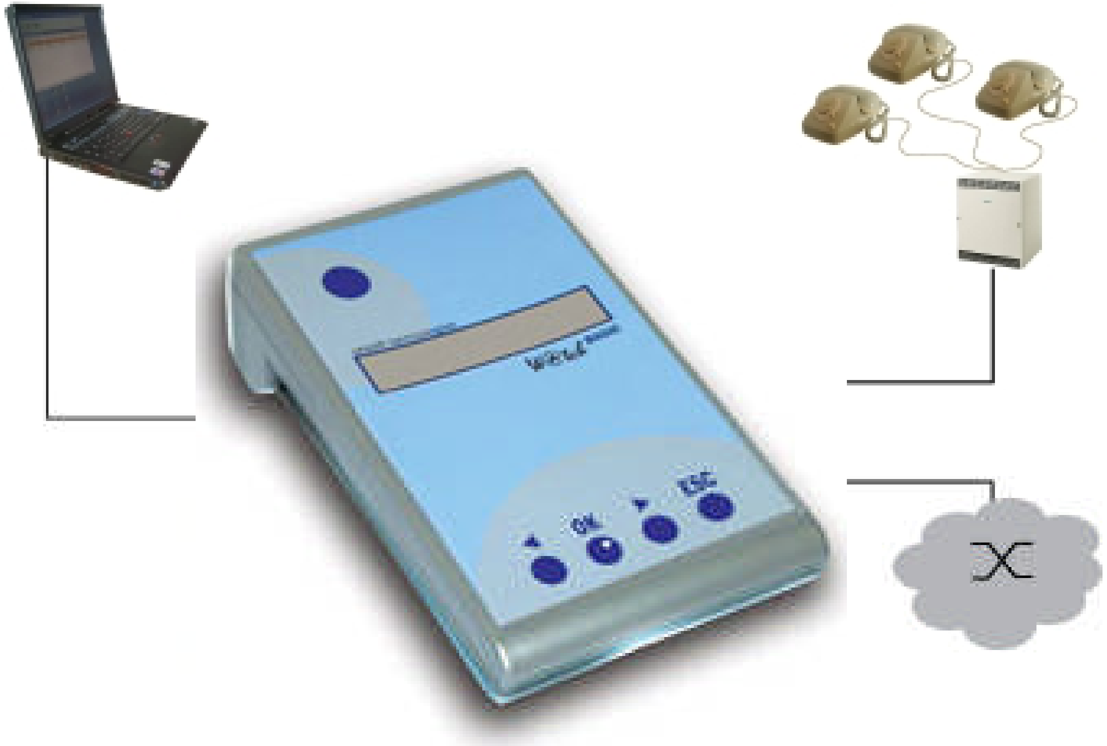


Wiretaps between the telephone line and the host



ISDN Protocol Analysis

- Stores messages passed between Merchant POS and Bank Host
- ISO8583 or derived protocol defines message structure
- PIN is encrypted



Criminals either hide unit on merchant premises (with collusion of staff) or hide unit in nearby local exchange

Digital MP3 players used for signal interception

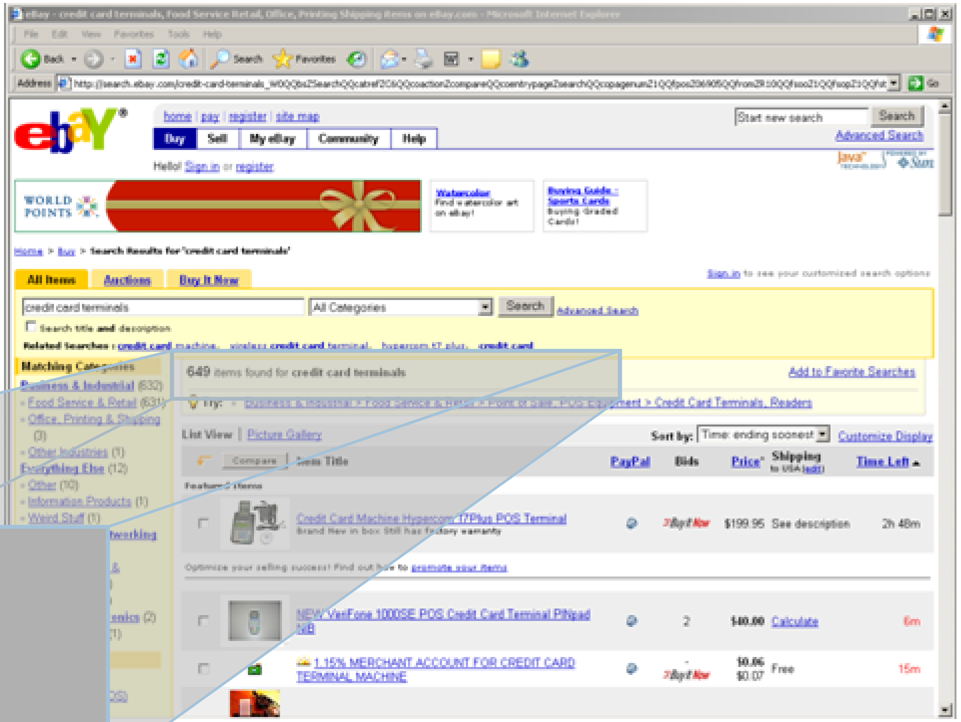
Obtaining a PIN by attacking the PED

To obtain and replace a PED, criminals often pretend to be a service engineer

Standard method of operation is to obtain two PEDs, one to learn where the security features are; the second, the target of the attack

The technology you need is readily available

Buy it from eBay



eBay - credit card terminals, Food Service Retail, Office, Printing Shipping items on eBay.com - Microsoft Internet Explorer

Address: http://search.ebay.com/credit-card-terminals_W0QQbsZSearchQQcatrefZC6QQcoactionZcompareQQcoentrypageZsearchQQcopagenumZ1QQfposZ06905QQfromZR10QQfsooZ1QQfsopZ1QQfst

Hello! Sign in or register

Home > Buy > Search Results for 'credit card terminals'

Sign in to see your customized search options

credit card terminals | All Categories | Search | Advanced Search

□ Search title and description

Related Searches : credit card machine, wireless credit card terminal, hypercom t7 plus, credit card

Matching Categories
- Business & Industrial (632)
  - Food Service & Retail (631)
  - Office, Printing & Shipping (3)
  - Other Industries (1)
- Everything Else (12)
  - Other (10)
  - Information Products (1)
  - Weird Stuff (1)

649 items found for credit card terminals

Add to Favorite Searches

Try: Business & Industrial > Food Service & Retail > Point of Sale, POS Equipment > Credit Card Terminals, Readers

List View | Picture Gallery

Sort by: Time: ending soonest | Customize Display

Featured Items

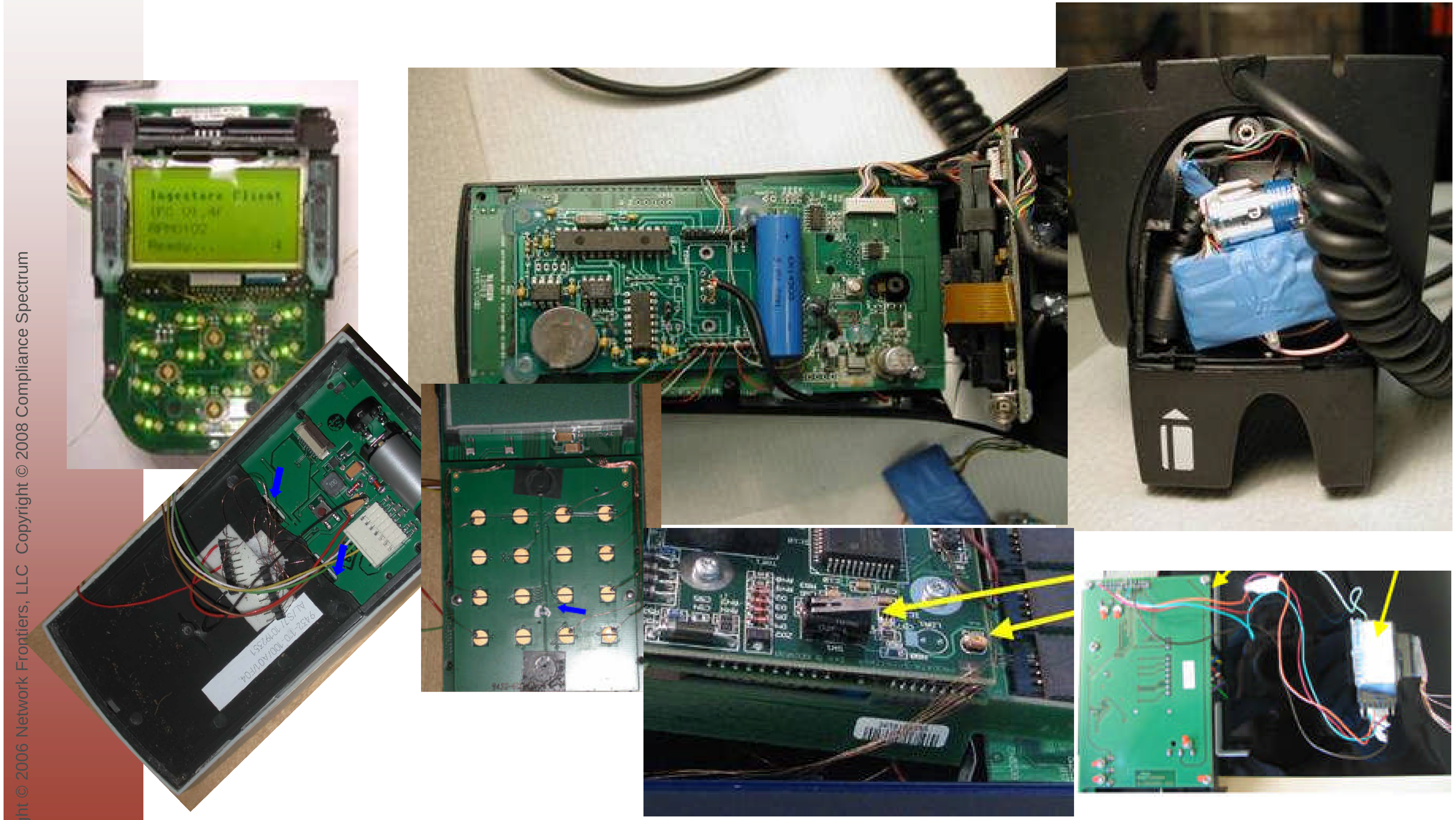
	Item Title	PayPal	Bids	Price	Shipping to USA (edit)	Time Left
□	Credit Card Machine Hypercom T7Plus POS Terminal Brand New in box Still has factory warranty		Buy It Now	$199.95	See description	2h 48m
□	NEW VeriFone 1000SE POS Credit Card Terminal PINpad NB		2	$40.00	Calculate	6m
□	1.15% MERCHANT ACCOUNT FOR CREDIT CARD TERMINAL MACHINE		- Buy It Now	$0.06 $0.07	Free	15m

Optimize your selling success! Find out how to promote your items

649 Terminals available,

All major vendors

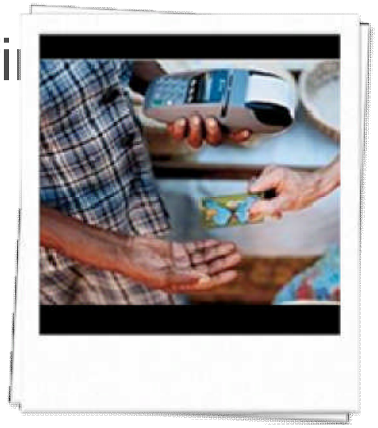
Criminals defeat security and insert skimming bugs



Observation of PIN entry

Visual Observation

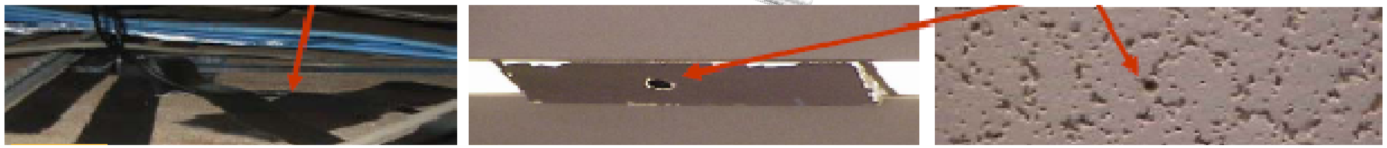
- Shoulder surfi
- Mini Camera



Micro Camera

Camera taped to ceiling tile

Very small holes required for camera



Choose your target carefully

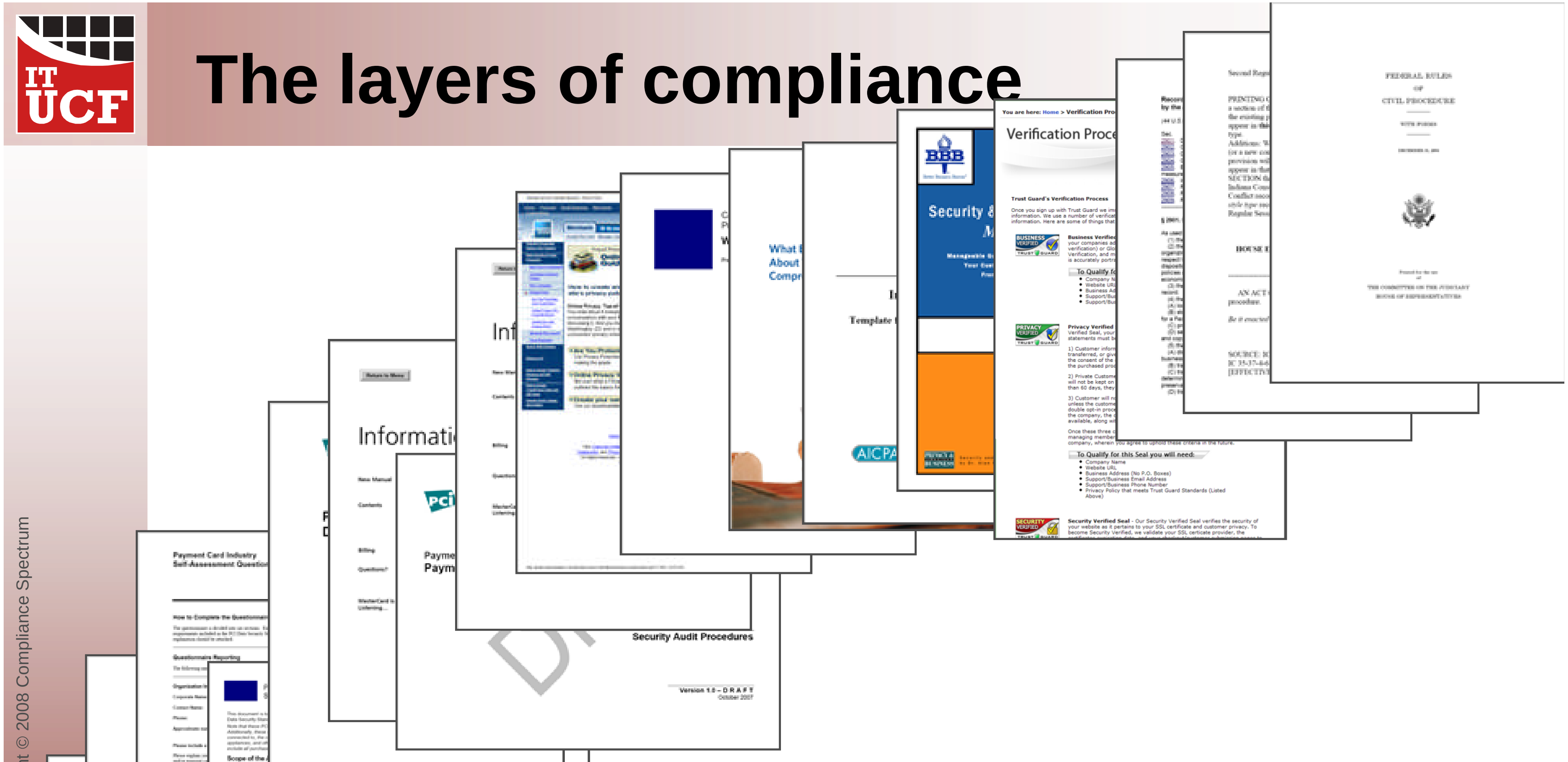
- Certain commonalities have begun to appear
  - Out of town location
  - Open extended hours
  - Limited number of staff on duty
  - Generally earning minimum wage
- Yet providing a good opportunity to obtain a large number of card details in a relatively short period
- Historically it was assumed that merchant staff would be the first line of defence but…

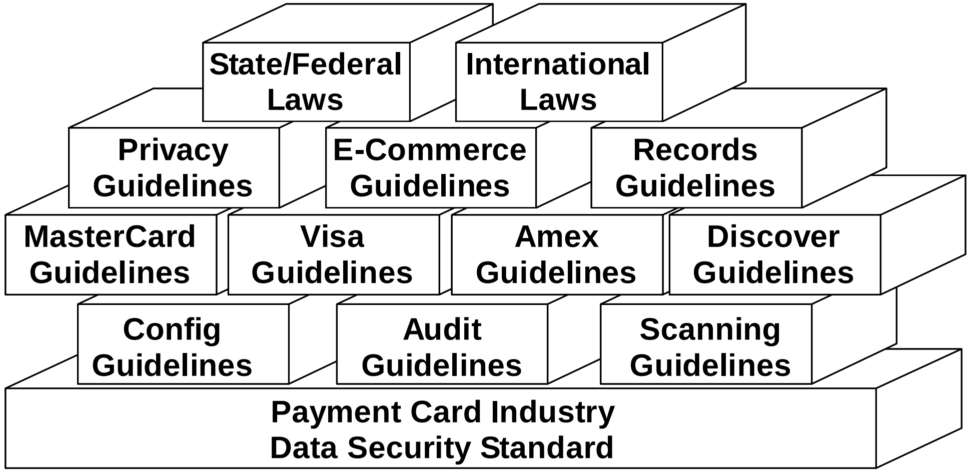
PED environmental risks

- Common issues with Merchant back end systems on three separate fraud cases
  - No clear logs of which terminal is in which location
  - No system checks on terminal status
  - System does not detect terminal being removed
  - System does not react to terminal being disconnected for a significant period
  - System also does not react to terminal being reconnected
  - System does not react if terminal appears in different location

Who should comply, and what does comply *really* mean?

The layers of compliance



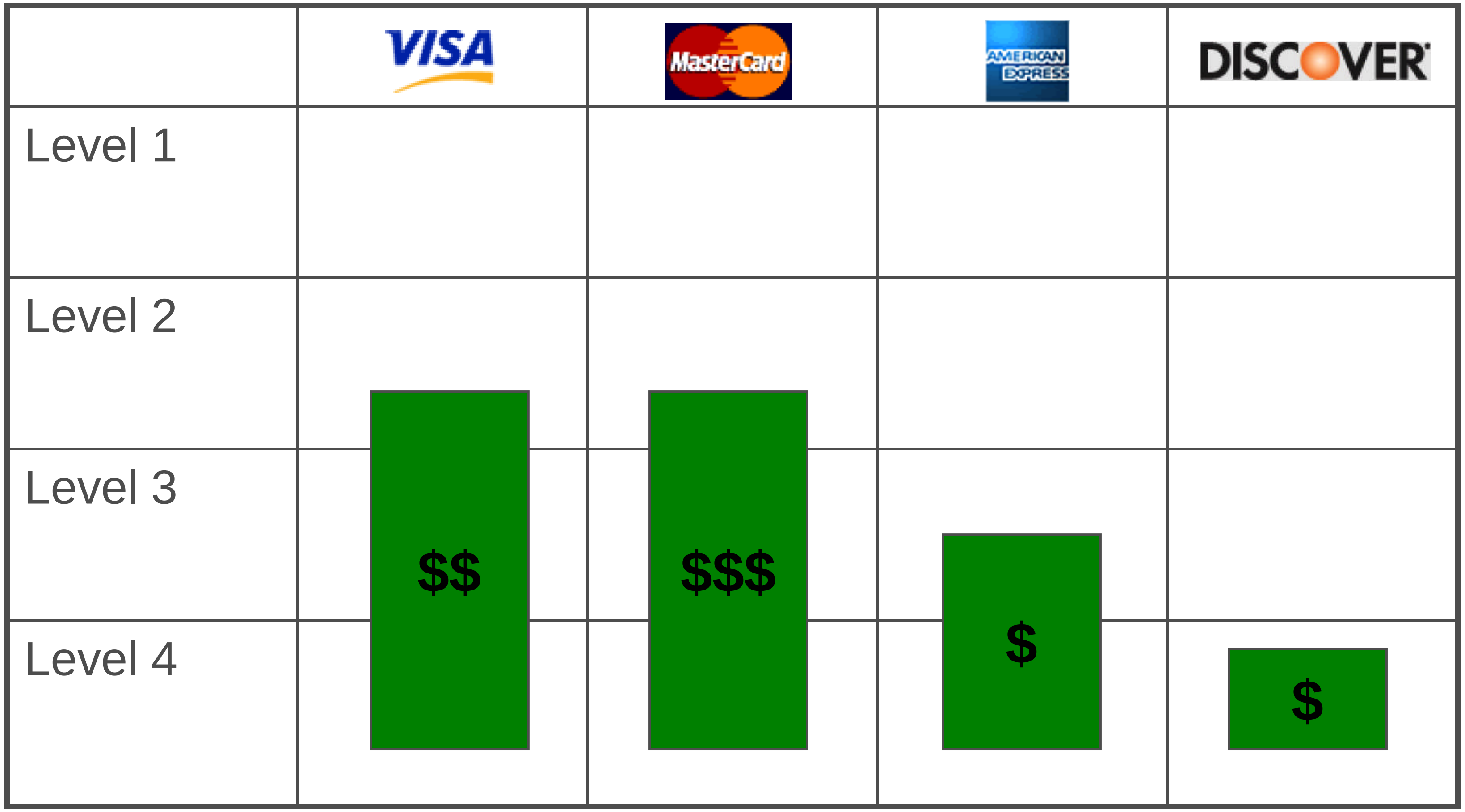


Who should comply?

- Anyone who takes credit card orders
  - Mail Order, Telephone Order (MOTO)
  - Point of Sale systems
  - E-commerce systems
- Size matters somewhat
  - There are 4 levels of PCI-DSS compliance, based upon the number of annual transactions
  - *There is no difference for any other contractual obligation*

- **PCI-DSS**
  - Level 1
    - >6 MM transactions
    - All TPPs
    - All DSEs storing data
    - Anyone compromised
  - Level 2
    - > 150,000 transactions
  - Level 3
    - > 20,000 transactions
  - Level 4
    - Everyone else

Your level of compliance



	VISA	MasterCard	AMERICAN EXPRESS	DISCOVER
Level 1				
Level 2				
Level 3	$$	$$$		
Level 4			$	$

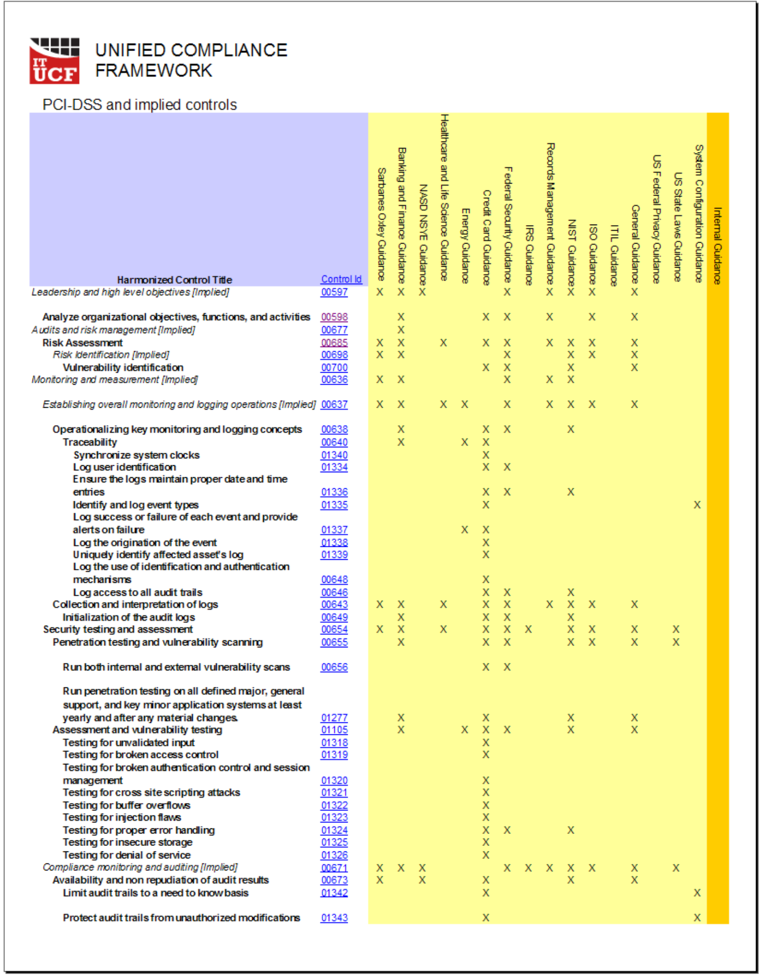
How should we comply with PCI-DSS?

Level	Requirement	
Level 1	3rd party Audit	Quarterly Network Scan
Level 2	Self Assessment	
Level 3		
Level 4		

What are the ~~PCI-DSS~~ requirements?
Payment Card Industry

- As stated earlier, there is the PCI-DSS standard and several others that have to be considered:
  - Applicable Configuration Management guidelines
  - Applicable auditing guidelines
  - Applicable scanning guidelines
  - Each card brand's reporting guidelines
  - Each card brand's additional guidelines (such as network architecture guidelines, incident response guidelines, etc.)
  - Additional commerce and privacy contractual guidelines
  - State, Federal, and international laws

Build and maintain a secure network	
Requirement 1	Install and maintain a firewall configura
Requirement 2	Do not use vendor-supplied defaults fo
Protect cardholder data	
Requirement 3	Protect stored data and do not sore ca
Requirement 4	Encrypt transmission of cardholder dat
Maintain a vulnerability management program	
Requirement 5	Use and regularly update antivirus soft
Requirement 6	Develop and maintain secure systems
Implement strong access control measures	
Requirement 7	Restrict access to data by business ne
Requirement 8	Assign a unique ID to each person wit
Requirement 9	Restrict physical access to cardholder
Regularly monitor and test networks	
Requirement 10	Track and monitor all access to networ
Requirement 11	Regularly test security systems and pr
Maintain and information security policy	
Requirement 12	Establish and maintain high level secu

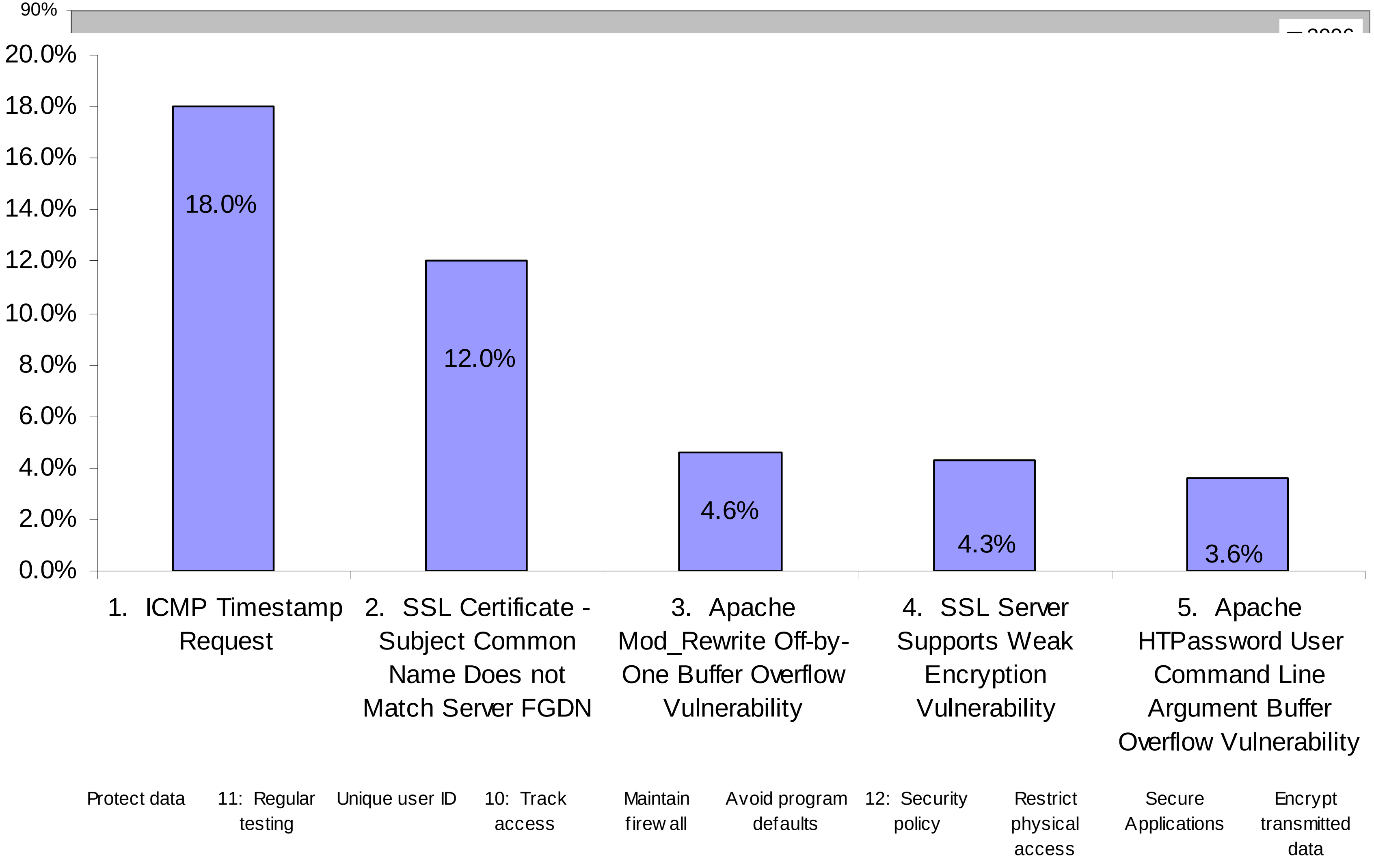


UNIFIED COMPLIANCE FRAMEWORK

PCI-DSS and implied controls

Harmonized Control Title	Control Id	Sarbanes Oxley Guidance	Banking and Finance Guidance	NASD NSYE Guidance	Healthcare and Life Science Guidance	Energy Guidance	Credit Card Guidance	Federal Security Guidance	IRS Guidance	Records Management Guidance	NIST Guidance	ISO Guidance	ITIL Guidance	General Guidance	US Federal Privacy Guidance	US State Laws Guidance	System Configuration Guidance	Internal Guidance
Leadership and high level objectives [Implied]	00597	X	X	X				X		X	X	X		X				
Analyze organizational objectives, functions, and activities	00598		X				X	X		X		X		X				
Audits and risk management [Implied]	00677		X															
Risk Assessment	00685	X	X		X		X	X		X	X	X		X				
Risk Identification [Implied]	00698	X	X					X			X	X		X				
Vulnerability identification	00700						X	X			X			X				
Monitoring and measurement [Implied]	00636	X	X					X		X	X							
Establishing overall monitoring and logging operations [Implied]	00637	X	X		X	X		X		X	X	X		X				
Operationalizing key monitoring and logging concepts	00638		X				X	X			X							
Traceability	00640		X			X	X											
Synchronize system clocks	01340						X											
Log user identification	01334						X	X										
Ensure the logs maintain proper date and time entries	01336						X	X			X							
Identify and log event types	01335						X										X	
Log success or failure of each event and provide alerts on failure	01337					X	X											
Log the origination of the event	01338						X											
Uniquely identify affected asset's log	01339						X											
Log the use of identification and authentication mechanisms	00648						X											
Log access to all audit trails	00646						X	X			X							
Collection and interpretation of logs	00643	X	X		X		X	X		X	X	X		X				
Initialization of the audit logs	00649		X				X	X			X							
Security testing and assessment	00654	X	X		X		X	X	X		X	X		X		X		
Penetration testing and vulnerability scanning	00655		X				X	X			X	X		X		X		
Run both internal and external vulnerability scans	00656						X	X										
Run penetration testing on all defined major, general support, and key minor application systems at least yearly and after any material changes.	01277		X				X				X			X				
Assessment and vulnerability testing	01105		X			X	X	X			X			X				
Testing for unvalidated input	01318						X											
Testing for broken access control	01319						X											
Testing for broken authentication control and session management	01320						X											
Testing for cross site scripting attacks	01321						X											
Testing for buffer overflows	01322						X											
Testing for injection flaws	01323						X											
Testing for proper error handling	01324						X	X			X							
Testing for insecure storage	01325						X											
Testing for denial of service	01326						X											
Compliance monitoring and auditing [Implied]	00671	X	X	X				X	X	X	X	X		X		X		
Availability and non repudiation of audit results	00673	X		X			X				X			X				
Limit audit trails to a need to know basis	01342						X										X	
Protect audit trails from unauthorized modifications	01343						X										X	

Where are merchants having problems?



Top Ten Vulnerabilities Sample Size: 85,000

- 10 - Telnet running
- 9 - Outdated Apache Mod_Frontpage
- 8 - Man-in-the-middle remote desktop attack
- 7 - Found telnet default password
- 6 - Outdated IIS
- 5 - Outdated OpenSSH
- 4 - Cross-Site Scripting
- 3 - Inconclusive Scan: (Port scan blocking at FW or IDS, or no required services present)
- 2 - Outdated SSH
- 1 - Using SSL version 2.0 (SAQ 4.2)

Which IT assets are in scope?

Which computing assets do the payment card industry guidelines cover, and which assets *don't they* cover?

PCI-DSS applies to all system assets/components that are *in scope*

Asset	Docs	Apps	OSes	Storage	Device	Network	Power	Facility
	Static & dynamic web pages Database tables (if they exist) Sales reports (optional) E-mail messages (optional)	Web server Application server Database engine CGI, JDBC, ODBC Scripts *Other utilities & apps*	Windows or Unix OSes integrated OSes in appliances	Anything from single drives through RAID arrays and network storage devices Tape or other removable media for backup	POS devices Kiosks Web servers DNS server Database server Mail server Firewalls Routers Switches NTP server Authentication server	Public Internet VPNs DMZ Secure DB subnet User's network Back-end secure subnet Wireless access	N/A in PCI-DSS	Data center Merchant's facility

System scoping overview

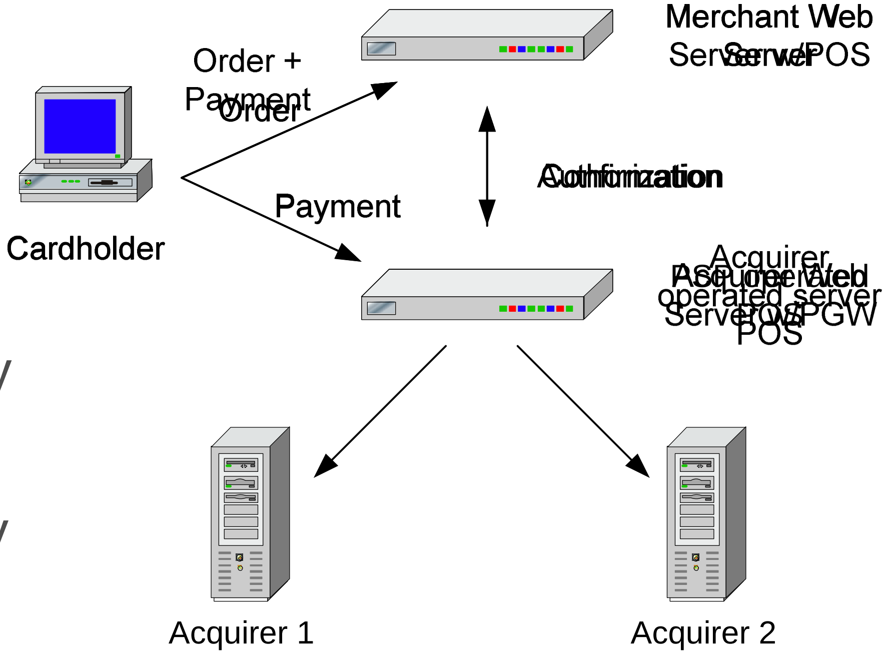
E-commerce sites are different than POS networks

- E-Commerce Fundamentals
  - Online payment configurations
  - E-Commerce modes of operation
- The POS systems
  - POS systems
  - Kiosks
  - In-store processor
  - LOB servers

- All sites have some common components
  - Border routers
  - Firewalls
  - The network
  - Authentication servers
  - DNS servers
  - Operating environments
  - Stored data
  - E-mail
  - Notebooks
  - Operational logs
  - *Users*

Online payment configurations

- There are three methods for implementing online payment.
- The merchant may:
  - Own the payment software
  - Use a server Point of Sale (POS) operated by an acquirer
  - Use a POS operated by a Payment Service Provider (PSP)

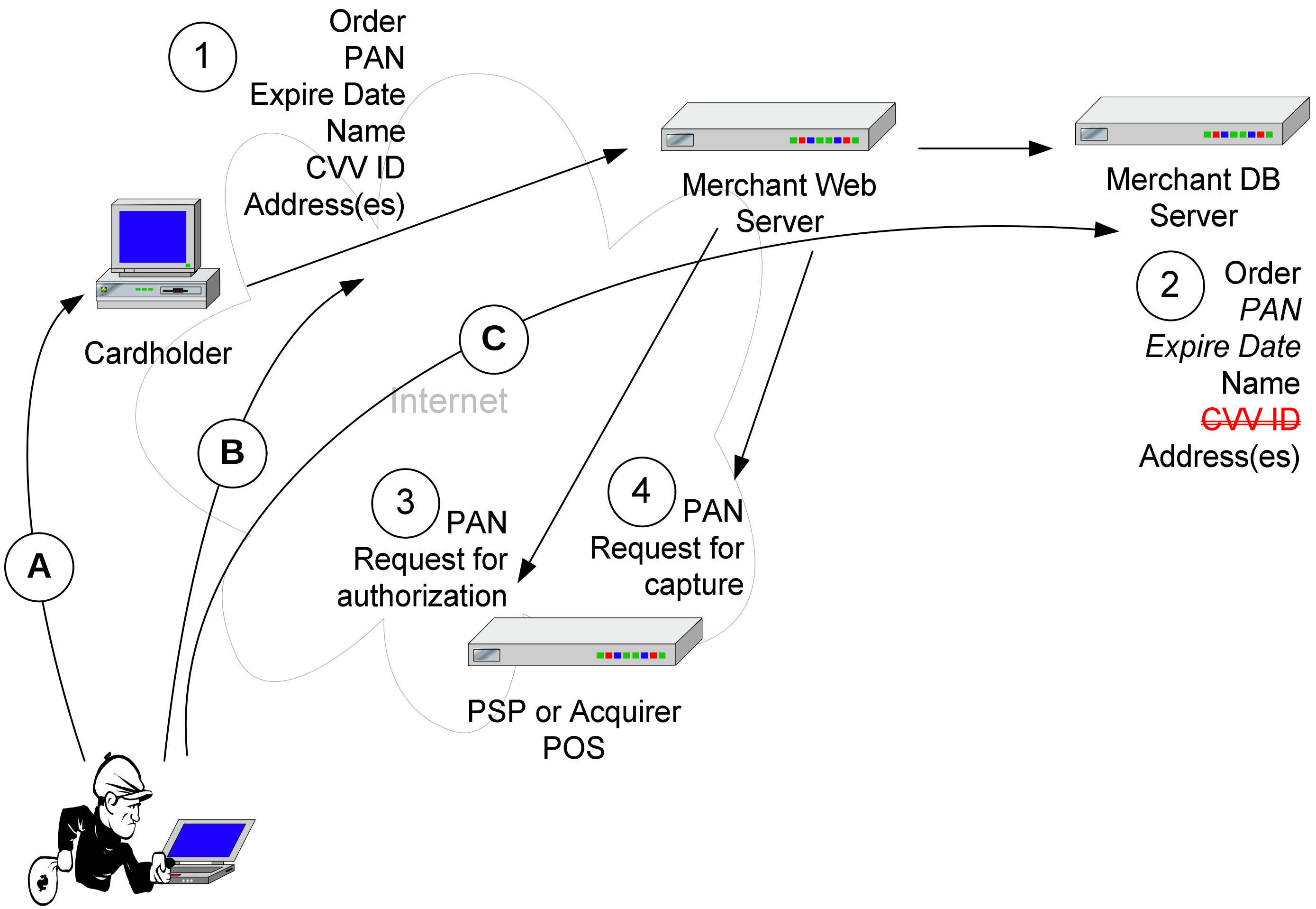


If the merchant doesn’t own the payment software

- When the e-commerce merchant does not own payment software, further action is necessary after the e-commerce transaction is complete.
  - Order treatment
  - Capture or refund

- Order treatment
  - Proper precautions are necessary to guarantee the confidentiality of the information during transit
- Capture or refund
  - The communication must be protected from eavesdropping

Security soft points for E-Commerce



E-Commerce configuration modes

- Dedicated
  - Dedicated configurations are those where the merchant has all equipment and software in-house
- Co-location
  - Co-located configurations are those where the merchant owns the server and the installed software, but the server is located in a data center of an Internet Service Provider (ISP)
- Hosting
  - Hosting is a merchant Web site operated by a third party
- Single box
  - The simplest architecture is a single box containing all the software required for the e-commerce environment
- Single box behind a firewall
  - Internet merchants often install a firewall between the box and the Internet to make the single box architecture more secure
- Multiple servers behind a firewall
  - Internet merchants often install a firewall between the box and the Internet to make the single box architecture more secure
- Multiple servers and multiple firewalls
  - In a multiple firewall configuration, an extra firewall increases the security. The extra firewall acts as an extra security layer. This means that if a compromise occurs on one layer, the other layer continues to protect

Single box system

Asset	Docs	Apps	OSes	Storage	Device	Network	Power	Facility
Web Server	Static & dynamic web pages Database tables (if they exist)	Web server Application server Database engine	Windows or Unix	Anything from single drives through RAID arrays	Single web server			

Single box behind a firewall system

Asset	Docs	Apps	OSes	Storage	Device	Network	Power	Facility
Firewall	Config file	Integrated	Integrated	None	Appliance			
Web Server	Static & dynamic web pages Database tables (if they exist)	Web server Application server Database engine	Windows or Unix	Anything from single drives through RAID arrays	Single web server	DMZ subnet		

Web server and separate database behind a firewall system

Asset	Docs	Apps	OSes	Storage	Device	Network	Power	Facility
Firewall	Config file	Integrated	Integrated	None	Appliance	Public (P1) DMZ (P2) Secure DB subnet (P3) User’s (P4)		
Web server	Static & dynamic web pages	Web server Application server ODBC or JDBC to DB server	Windows or Unix	Anything from single drives through RAID arrays	Single server	DMZ subnet		
Database server	Data tables	Database engine	Windows or Unix	Same as above	Usually a single server	Secure DB subnet		

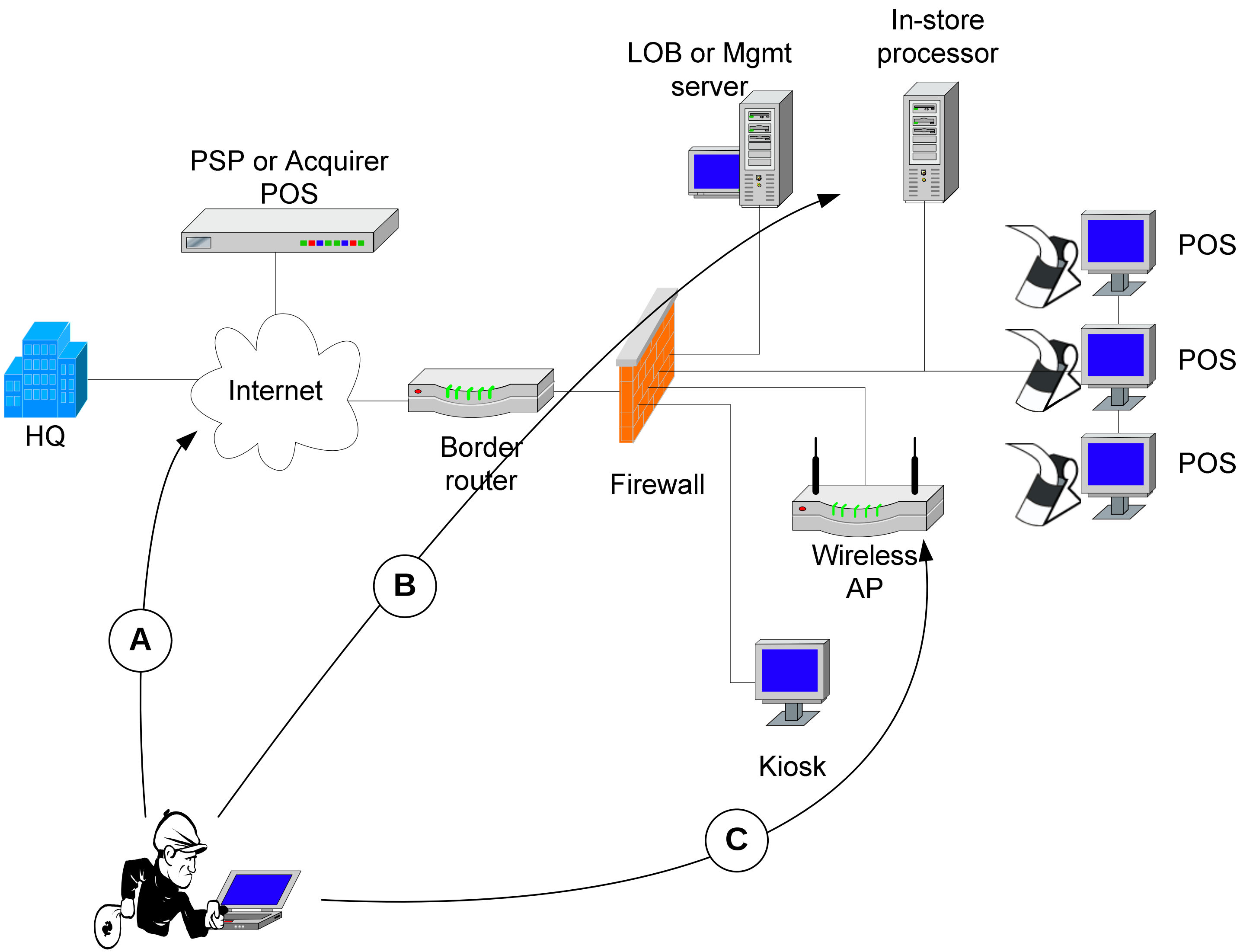
Multiple firewall configuration system

Asset	Docs	Apps	OSes	Storage	Device	Network	Power	Facility
Firewall 1	Config file	Integrated	Integrated	None	Appliance	Public (P1) DMZ (P2) Direct (P3)		
Firewall 2	Config file	Integrated	Integrated	None	Appliance	Direct (P1) Secure DB subnet (P2) User's (P3)		
Web server	Static & dynamic web pages	Web server Application server ODBC or JDBC to DB server	Windows or Unix	Anything from single drives through RAID arrays	Single server	DMZ subnet		
Database server	Data tables	Database engine	Windows or Unix	Same as above	Usually a single server	Secure DB subnet		

POS (retail/hospitality) system

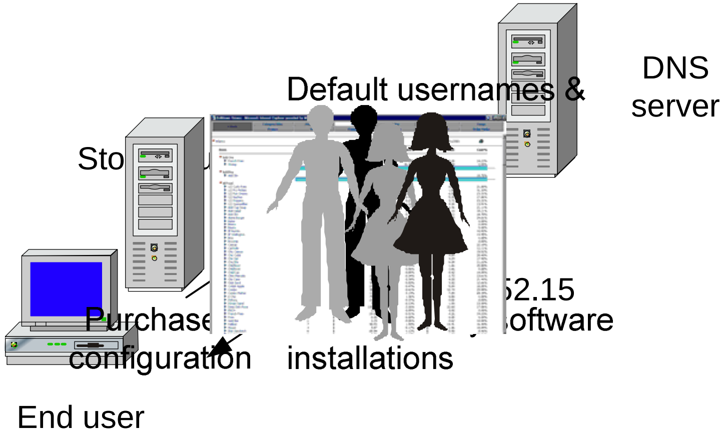
Asset	Docs	Apps	OSes	Storage	Device	Network	Power	Facility
Border router	Config file	Integrated	Integrated	None	Appliance	Public (P1) FW (P2)		
Firewall	Config file	Integrated	Integrated	None	Appliance	BR (P1) Mgmt (P2) POS (P3) Wireless (P4) Kiosks (P5)		
Wireless AP	Config file	Integrated	Integrated	None	Appliance	FW (P1) Users (P2)		
POS & Kiosks	Config file	Integrated	Integrated	None	Appliance	POS or Kiosk		
In-store processor	Data tables & cc transactions	Database engine POS Application	Windows or Unix	Anything from single drives through RAID arrays	Usually a single computing device	POS subnet		
LOB or Mgmt server	Misc. reports, personnel info	Scheduling, inventory, HR, GL	Windows or Unix	Anything from single drives through RAID arrays	Usually a single computing device	Mgmt secure subnet		

Security soft points for POS



Additional common elements

- DNS servers
- “out of the box” operating environments
- E-mail
- Mobile computers
- Operational logs
- Users



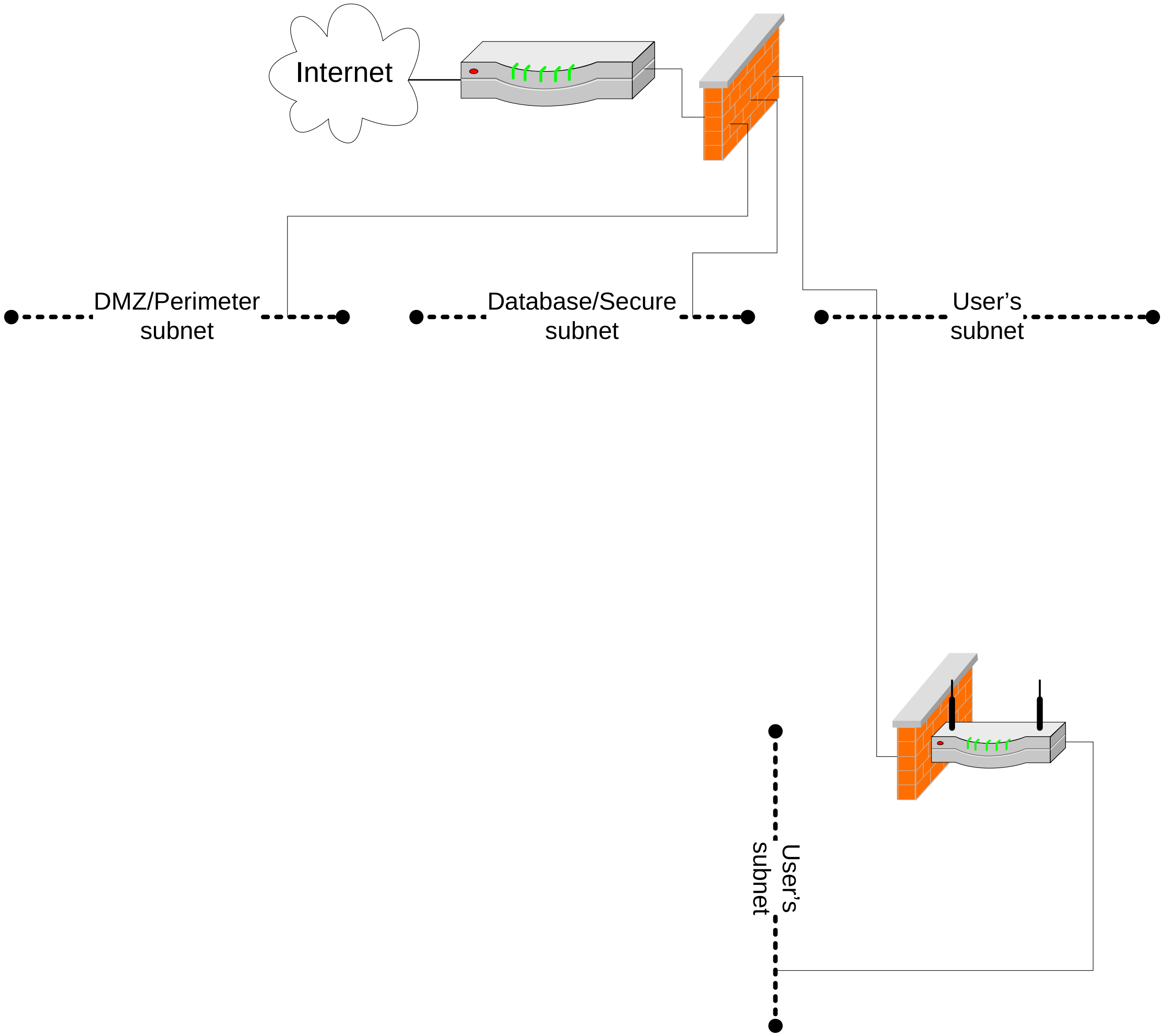
Build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Securing the network overview

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

1 Install and maintain a firewall configuration



1.1 Establish firewall configuration standards

- SonicWALL suggests that the organization turn to their policies, standards, and procedures for proper documentation before staging and “making live” any firewall products.

1.1.3 Requirements for a firewall at each Internet connection and between any DMZ and the intranet

- **SonicWALL GMS** Pg 155 states that firewall configuration of network zones, VLANs, or SonicWALL PortShield services could be enforced using GMS.
- **SonicWALL OS Standard** Pg 61 states that SonicOS Standard supports firewalling between the DMZ, Internet and the internal LAN network.
- **SonicWALL SonicOS Enhanced** Pg 71 states that VLAN support and Portshield allow for zone segmentation on a single unit with SonicOS Enhanced firmware.

1.1.5 Documented list of services/ports necessary for business

- **SonicWALL SSL-VPN** Vendor Note states that the usage of SSL-VPN services (port 443 or otherwise) for remote access must be documented.
- **SonicWALL EMS** Vendor Note states that the administrator should document the usage of SMTP (25), SSL/TLS (443), or any reserved or non-reserved ports used for EMS, Proxy, or MTA services.
- **SonicWALL CDP** Vendor Note states that the administrator should ports used by CDP Enterprise manager (e.g. Unreserved port 10001).

1.1.6 Justification and documentation for any available protocols (other than the basics)

- **SonicWALL SSL-VPN** Vendor Note states that the administrator must specify port(s) for SSL-VPN remote access services.
- **SonicWALL EMS** Vendor Note states that the administrator must specify port(s) for E-mail Security services.
- **SonicWALL CDP** Vendor Note states that the administrator must specify ports used by CDP Enterprise manager (e.g. Unreserved port 10001).

1.2 Deny all traffic from untrusted networks and hosts

- **SonicWALL GMS** Pg 158 states that this is a part of the default configuration.
- **SonicWALL SonicOS Enhanced** Pgs 302, 304 states that this is a part of the default configuration.

1.3 Build a firewall configuration that restricts connections

- **1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:**
- 1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)
- 1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443
- 1.3.3 Not allowing internal addresses to pass from the Internet into the DMZ (egress filters)
- 1.3.4 Stateful inspection, also known as dynamic packet filtering (only ”established” connections are allowed into the network)
- 1.3.5 Placing the database in an internal network zone, segregated from the DMZ
- 1.3.6 Restricting outbound traffic to that which is necessary for the payment card environment
- 1.3.7 Securing and synchronizing router configuration files (e.g., running configuration files – used for normal running of the routers, and start-up configuration files - used when machines are re-booted, should have the same, secure configuration).
- 1.3.8 Denying all other inbound and outbound traffic not specifically allowed
- 1.3.9 Installation of perimeter firewalls between any wireless networks and the payment card environment, and configuration of these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment
- 1.3.10 Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization’s network

1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)

- **SonicWALL OS Standard** Pg 177 states that this is a part of the default configuration.
- **SonicWALL SonicOS Enhanced** Pgs 106 - 108 states that this is already a part of the default configuration.

1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443

- **SonicWALL OS Standard** Vendor Note states that this is a part of the default configuration.
- **SonicWALL SonicOS Enhanced** Vendor Note states that this is a part of the default configuration.

1.3.3 Not allowing internal addresses to pass from the Internet into the DMZ

- **SonicWALL SonicOS Standard** Vendor Note states that this is default behavior of the SonicWALL Deep Packet Inspection (DPI) engine.
- **SonicWALL SonicOS Enhanced** Vendor Note states that this is default behavior of the SonicWALL Deep Packet Inspection (DPI) engine.

1.3.6 Restricting outbound traffic to that which is necessary for the payment card environment

- **SonicWALL GMS** Vendor Note states that this can be managed for other SonicOS products through GMS.
- **SonicWALL OS Standard** Vendor Note states that SonicWALL units only keep a single previous configuration file on the native device. Authenticated access is required for viewing, manipulation or exportation.
- **SonicWALL SonicOS Enhanced** Vendor Note states that SonicWALL units only keep a single previous configuration file on the native device. Authenticated access is required for viewing, manipulation or exportation.
- **SonicWALL SSL-VPN** Vendor Note states that SonicWALL SSL-VPN 2000 & 4000 units only keep a single previous configuration file on the native device (this does not apply to the SSL-VPN 200). Authenticated access is required for viewing, manipulation or exportation.
- **Additional SonicWALL info:** SonicWALL devices can have one previous configuration file stored on the device. The only exception are the PRO 4060 and higher devices, which have the capability of storing two previous configurations on the native device. If GMS is used in an installation, there is no hard limit to the number of previous configurations.

1.3.7 Securing and synchronizing router configuration files

- **SonicWALL GMS** Pg 158 states that this is a part of the default configuration.
- **SonicWALL SonicOS Enhanced** Pgs 302, 304 states that this is a part of the default configuration.

1.4 Prohibit direct public access to cardholder data

- **SonicWALL GMS** Vendor Note states that GMS maintains the default "denial-all" policy from the WAN interface to everything internal to the network.
- **SonicWALL OS Standard** Vendor Note states that the default configuration has a "denial-all" rule from the WAN interface to everything internal to the network.
- **SonicWALL SonicOS Enhanced** Pg 99; Pgs 146 - 147 states that there is already a a denial-all from the WAN to everything internal to the network.
- **SonicWALL SSL-VPN** Vendor Note states that there is already an inherent "denial-all" policy when configured behind a SonicWALL Firewall.

1.5 Implement NAT and PAT

- **SonicWALL OS Standard** this is a default feature of all firewall products.
- **SonicWALL SonicOS Enhanced** this is a default feature of all firewall products.

2 Do not use default passwords and accounts

- **2.1 Always change the vendor-supplied defaults before you install a system on the network (e.g., passwords, SNMP community strings, and elimination of unnecessary accounts).**
- 2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, WEP keys, default SSID, passwords, and SNMP community strings, and disabling of SSID broadcasts. Enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.
- 2.2 Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices
- 2.2.1 Implement only one primary function per server (e.g., web servers, database servers, and DNS should be implemented on separate servers)
- 2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).
- 2.2.3 Configure system security parameters to prevent misuse
- 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g., unnecessary web servers).
- 2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

2.2.1 Implement only one primary function per server

- **SonicWALL GMS** Vendor Note states that optimal configuration for GMS is on a distributed server environment. At minimum, GMS (console, Agent, Summarizer) should be installed on a dedicated machine. The GMS Database should be installed on a separate machine.
- **SonicWALL EMS** Vendor Note states that the optimal configuration would be to have a dedicated server for the software version of EMS. Configuration with the EMS software application and Microsoft Exchange would be recommended.
- **SonicWALL CDP** Vendor Note states that optimal configuration is to have the CDP Enterprise Manager installed on a dedicated server.

2.2.2 Disable all unnecessary and insecure services and protocols

- **SonicWALL GMS** Vendor Note states that only the necessary GMS components should be running on a dedicated GMS Server. For example, IIS, SSH, and DHCP should be disabled.
- **SonicWALL EMS** Vendor Note states that only the necessary GMS components should be running on a dedicated GMS Server. For example, IIS, SSH, and DHCP should be disabled.
- **SonicWALL CDP** Vendor Note states that only the necessary GMS components should be running on a dedicated GMS Server. For example, IIS, SSH, and DHCP should be disabled.

2.3 Encrypt all non-console administrative access

- **SonicWALL GMS** Vendor Note states that the administrator must prescribe an HTTP configuration. Provide pointer to HTTPS management on GMS.
- **SonicWALL OS Standard** Vendor Note states that the administrator must provide pointer to administrative configuration to enable/disable HTTP/HTTPS.
- **SonicWALL SonicOS Enhanced** Vendor Note states that the administrator must provide pointer to administrative configuration to enable/disable HTTP/HTTPS.
- **SonicWALL SSL-VPN** Vendor Note states that the administrator must provide pointer to administrative configuration to enable/disable HTTP/HTTPS.
- **SonicWALL EMS** Vendor Note states that the administrator must provide pointer to administrative configuration to enable/disable HTTP/HTTPS.
- **SonicWALL CDP** Vendor Note states that the administrator must provide pointer to administrative configuration to enable/disable HTTP/HTTPS.

Protect Cardholder data

3. Protect stored data

4. Encrypt transmission of cardholder data and sensitive information across public networks

Protecting Cardholder data overview

Cardholder data is the target of attack and must be protected

- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks

3.1 Keep cardholder information storage to a minimum

- **3.1 Keep cardholder information storage to a minimum.**
  - **Develop a data retention and disposal policy.**
  - **Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.**

3.2 Do not store sensitive authentication data subsequent to authorization

- **3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted):**
- 3.2.1 Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.)
- 3.2.2 Do not store the card-validation code (Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data))
- 3.2.3 Do not store the PIN Verification Value (PVV)

3.3 Mask account numbers when displayed

- **3.3 Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed).**
  - **Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.**

3.4 Render sensitive cardholder data unreadable anywhere it is stored

- **SonicWALL CDP** Vendor Note states that if CDP is being used for backup/recovery services to the POS system, content encryption should be used. Policy should be to have encryption at the local level before backup to CDP or offsite storage.

3.5 Protect encryption keys against both disclosure and misuse

- **3.5 Protect encryption keys against both disclosure and misuse.**
- 3.5.1 Restrict access to keys to the fewest number of custodians necessary
- 3.5.2 Store keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key management processes and procedures

- **3.6 Fully document and implement all key management processes and procedures, including:**
- 3.6.1 Generation of strong keys
- 3.6.2 Secure key distribution
- 3.6.3 Secure key storage
- 3.6.4 Periodic key changes
- 3.6.5 Destruction of old keys
- 3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).
- 3.6.7 Prevention of unauthorized substitution of keys
- 3.6.8 Replacement of known or suspected compromised keys
- 3.6.9 Revocation of old or invalid keys (mainly for RSA keys)
- 3.6.10 Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities

4.1 Use strong cryptography and encryption techniques

- **4.1 Use strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks**

- 4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless LAN.
- Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.

4.2 Never send cardholder information via unencrypted e-mail

- **4.2 Never send cardholder information via unencrypted e-mail.**

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Maintain a Vulnerability Management Program Preview

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

5.1 Deploy anti-virus mechanisms

- **SonicWALL GMS** Vendor Note states that GMS can help ensure that this is set up correctly.
- **SonicWALL OS Standard** Vendor Note states that SonicWALL adheres a multi-layer security approach for anti-virus protection, which consists of GAV and Client AV services.
- **SonicWALL SonicOS Enhanced** Pgs 507 - 512; Pgs 545 - 552 states that SonicWALL adheres a multi-layer security approach for anti-virus protection, which consists of GAV and Client AV services.
- **SonicWALL EMS** Vendor Note states that SonicWALL adheres a multi-layer security approach for anti-virus protection, which consists of a client AV solution along with the AV services of the EMS server/ appliance.

5.2 Ensure that all anti-virus mechanisms are current

- **SonicWALL GMS** Vendor Note states that GMS helps to ensure all AV services can be patched.
- **SonicWALL OS Standard** Vendor Note states that SonicWALL can do network AV enforcement.
- **SonicWALL SonicOS Enhanced** Vendor Note states that SonicWALL can do network AV enforcement.
- **SonicWALL EMS** Vendor Note states that network AV support for EMS is constantly updating signatures.
- **Additional vendor note:** SonicWALL's Anti-Virus signature system is continuously monitored and updated.

6.1 Ensure that all system components and software have the latest vendor-supplied security patches

- **SonicWALL GMS** Vendor Note states that GMS automatically notifies the admin of an available patch or firmware.
- **SonicWALL OS Standard, Enhaned** Vendor Note states that the administrator must periodically check Mysonicwall.com for security advisories and new firmware availability.
- **SonicWALL SSL-VPN** Vendor Note states that he administrator must periodically check Mysonicwall.com for security advisories and new firmware availability.
- **SonicWALL CSM, EMS, CDP** Vendor Note states that he administrator must periodically check Mysonicwall.com for security advisories and new firmware availability.

6.2 Establish a process to identify newly discovered security vulnerabilities

- 6.2 Establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.

6.3 Develop software applications based on industry best practices

- **SonicWALL GMS** Vendor Note states that the administrator should stage test systems before adding units under GMS management.
- **SonicWALL OS Standard and Enchaned** Vendor Note states that the administrator should stage deployment for test systems.
- **SonicWALL SSL-VPN** Vendor Note states that the administrator should stage deployment for test systems.
- **SonicWALL CSM, EMS, and CDP** Vendor Note states that the administrator should stage deployment for test systems.

6.4 Follow change control procedures for all system and software configuration changes

- **SonicWALL GMS** Vendor Note states that GMS Provides back-out capabilities and the ability to backup an unlimited number of configurations.
- **SonicWALL OS Standard** Vendor Note states that SonicOS provides one past configuration
- **SonicWALL SonicOS Enhanced** Vendor Note states that SonicOS provides one past configuration. PRO 4060 and above units have two past configurations.
- **SonicWALL SSL-VPN** Vendor Note states that Sonic SSL-VPN 2000/4000 (not 200) firmware provides one past configuration Note that for the SSL-VPN 200 you can export settings and save it somewhere else as a backup.
- **SonicWALL CSM, EMS, and CDP** Vendor Note states that Sonic CSM firmware provides one backup configuration.

6.5 Develop web software and applications based on secure coding guidelines

- **6.5 Develop web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines.**
- **Review custom application code to identify coding vulnerabilities. See www.owasp.org - “The Ten Most Critical Web Application Security Vulnerabilities.”**
- **Cover prevention of common coding vulnerabilities in software development processes, to include:**
- 6.5.1 Unvalidated input
- 6.5.2 Broken access control (e.g., malicious use of user IDs)
- 6.5.3 Broken authentication/session management (use of account credentials and session cookies)
- 6.5.4 Cross-site scripting (XSS) attacks
- 6.5.5 Buffer overflows
- 6.5.6 Injection flaws (e.g., SQL injection)
- 6.5.7 Improper error handling
- 6.5.8 Insecure storage
- 6.5.9 Denial of service
- 6.5.10 Insecure configuration management.

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

Implement Strong Access Control Measures preview

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

7.1 Limit access to computing resources and cardholder information

- 7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access

- 7.2 Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

8.1 Identify all users with a unique username

- **SonicWALL Products note:** User-level authentication for remote access through the SonicWALL is supported with local RADIUS LDAP and AD authentication as our 2-factor authentication methods and CA based authentication. SSL-VPN allows for granular access control policies.

8.2 Employ multifactor authentication

- **SonicWALL GMS** Pg 764 states that GMS would leverage the authentication methods of managed firewalls. GMS itself has a password scheme for access to the web console.
- **SonicWALL OS Standard** Pg 236 states that this can be managed using user authentication methods defined by SonicOS.
- **SonicWALL SonicOS Enhanced** Pgs 448 - 462; Pgs 465-467 states that this can be managed using user authentication methods defined by SonicOS.
- **SonicWALL Products note:** User-level authentication for remote access through the SonicWALL is supported with local RADIUS LDAP and AD authentication as our 2-factor authentication methods and CA based authentication. SSL-VPN allows for granular access control policies.

8.3 Implement 2-factor authentication for remote access

- 8.3 Implement 2-factor authentication for remote access to the network by employees, administrators, and third parties.
- Use technologies such as RADIUS or TACOS with tokens, or VPN with individual certificates.

8.4 Encrypt all passwords

- 8.4 Encrypt all passwords during transmission and storage, on all system components.

8.5 Ensure proper user authentication and password management

- **8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components:**
- 8.5.1 Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- 8.5.2 Verify user identity before performing password resets.
- 8.5.3 Set first-time passwords to a unique value per user and change immediately after first use
- 8.5.4 Immediately revoke accesses of terminated users.
- 8.5.5 Remove inactive user accounts at least every 90 days
- 8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed
- 8.5.7 Distribute password procedures and policies to all users who have access to cardholder information
- 8.5.8 Do not use group, shared, or generic accounts/passwords
- 8.5.9 Change user passwords at least every 90 days
- 8.5.10 Require a minimum password length of at least seven characters
- 8.5.11 Use passwords containing both numeric and alphabetic characters
- 8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts
- 8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID
- 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
- 8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts

- **SonicWALL SonicOS Enhanced** Pgs 57 - 58 states that has this feature built in.

8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID

- **SonicWALL SonicOS Enhanced** Pgs 462 - 463 states that the SonicOS Enhanced 4.0 version has this feature built in.

more than 15 minutes, require the user to re-enter the password to re-activate the terminal

- **SonicWALL GMS** Pg 784 states that this is a supported option. Within GMS the idle time can be set between the default (10 minutes) to 120 minutes.
- **SonicWALL OS Standard** Pg 170 states that this is directly supported.
- **SonicWALL SonicOS Enhanced** Pgs 462 - 463 states that this is directly supported.

9.1 Use appropriate facility entry controls

- **9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.**
- 9.1.1 Use cameras to monitor sensitive areas. Audit this data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
- 9.1.2 Restrict physical access to publicly accessible network jacks.
- 9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.

9.2 Develop identification procedures

- 9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.
- “Employee” refers to full-time and part-time employees, temporary employees/personnel, and consultants who are “resident” on the entity’s site.
- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

9.3 Identify and track visitors

- **9.3 Make sure all visitors are:**
- 9.3.1 Authorized before entering areas where cardholder data is processed or maintained
- 9.3.2 Given a physical token (e.g., badge or access device) that expires, and that identifies them as non-employee
- 9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4 Use a visitor log

- 9.4 Use a visitor log to retain a physical audit trail of visitor activity.
- Retain this log for a minimum of three months, unless otherwise restricted by law.

9.5 Store media back-ups in a secure off-site facility

- **SonicWALL CDP** Vendor Note states that offsite storage with CDP services provides an encrypted transport to the backend.

9.6 Physically secure all paper and electronic media

- 9.6 Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.

9.7 Maintain strict control over sensitive media

- **9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information**
- 9.7.1 Label the media so it can be identified as confidential.
- 9.7.2 Send the media via secured courier or a delivery mechanism that can be accurately tracked.

9.8 Ensure management approves all media that is moved

- 9.8 Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).

9.9 Maintain strict control over media storage

- **9.9 Maintain strict control over the storage and accessibility of media that contains cardholder information:**
- 9.9.1 Properly inventory all media and make sure it is securely stored.

9.10 Destroy media when appropriate

- **9.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons:**
- 9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials
- 9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes.

Regularly monitor and test networks preview

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes.

10.1 Establish a process for linking all access to system components

- **SonicWALL GMS** Pg 764 requires either user level or role-based access.
- **SonicWALL SonicOS Enhanced** Vendor Note states that multiple administrative logins are available in SonicOS enhanced 4.0

10.2 Implement automated audit trails

- **All SonicWALL products** log both *all* user and administrator activity.

10.3 Record key audit trail entries

- **All SonicWALL products** log both *all* user and administrator activity.

10.4 Synchronize all critical system clocks

- **All SonicWALL products** Vendor Note all SonicWALL products can be synchronized with NTP.

10.5 Secure audit trails

- **SonicWALL GMS** Pg 785 states that this is a part of administrative access implementation.

10.6 Review logs for all system components at least daily

- **SonicWALL GMS** Pg 719 states that this should be done as a best practice.

10.7 Retain your audit trail history

- **SonicWALL GMS** Pg 769 states that the SonicOS has a limitation of 32K of logging data. Once this is “full,” it can be e-mailed to someone for further retention.

11.1 Test security controls, limitations, network connections, and restrictions

- 11.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts.
- Where wireless technology is deployed, use a wireless analyzer periodically to identify all wireless devices in use.

11.2 Run internal and external network vulnerability scans

- 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Note that external vulnerability scans must be performed by a scan vendor qualified by the payment card industry.

11.3 Perform penetration testing on network infrastructure and applications

- 11.3 Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment).

11.4 Use network and host-based intrusion detection/prevention systems

- 11.4 Use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.
- Keep all intrusion detection and prevention engines up to date.

11.5 Deploy file integrity monitoring

- 11.5 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated).
- *Critical files are not necessarily those containing cardholder data.*
- *File integrity monitoring products usually come pre-configured with critical files for the related operating system.*
- *For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise.*
- *Other critical files, such as those for custom applications, must be evaluated and defined by the merchant or service provider.*

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Maintain an Information Security Policy preview

- Maintain a policy that addresses information security

12.1 Establish, publish, maintain, and disseminate a security policy

- **12.1 Establish, publish, maintain, and disseminate a security policy that:**
- 12.1.1 Addresses all requirements in this specification.
- 12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment
- 12.1.3 Includes a review at least once a year and updates when the environment changes.

12.2 Develop daily operational security procedures

- **12.2 Develop daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, log review procedures)**

12.3 Develop usage policies

- **12.3 Develop usage policies for critical employee-facing technologies, such as modems and wireless, to define proper use of these technologies for all employees and contractors. Ensure these usage policies require:**
- 12.3.1 Explicit management approval
- 12.3.2 Authentication for use of the technology
- 12.3.3 A list of all such devices and personnel with access
- 12.3.4 Labeling of devices with owner, contact information, and purpose
- 12.3.5 Acceptable uses of the technology
- 12.3.6 Acceptable network locations for these technologies
- 12.3.7 A list of company-approved products
- 12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity
- 12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.
- 12.3.10 When accessing cardholder data remotely via modem, disable storage of cardholder data onto local hard drives, floppy disks or other external media. Also disable cut-and paste, and print functions during remote access.

12.4 Ensure the security policy and procedures define responsibilities

- 12.4 Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.

12.5 Assign responsibilities to users or teams

- **12.5 Assign to an individual or team the following information security management responsibilities:**
- 12.5.1 Establish, document, and distribute security policies and procedures
- 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel
- 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situation
- 12.5.4 Administer user accounts, including additions, deletions, and modifications
- 12.5.5 Monitor and control all access to data.

12.6 Make all employees aware

- **12.6 Make all employees aware of the importance of cardholder information security**
- 12.6.1 Educate employees (e.g., through posters, letters, memos, meetings, and promotions).
- 12.6.2 Require employees to acknowledge in writing they have read and understood the company's security policy and procedures.

12.7 Screen potential employees

- 12.7 Screen potential employees to minimize the risk of attacks from internal sources.
- For those employees who only have access to one card number at a time to facilitate a transaction, such as store cashiers, this requirement is a recommendation only.

12.8 Contractually require all third parties to your security requirements

- **12.8 Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address:**
- 12.8.1 Acknowledgement that the 3rd party is responsible for security of cardholder data in their possession.
- 12.8.2 Ownership by each Payment Card brand, Acquirer, and Merchants of cardholder data and acknowledgement that such data can ONLY be used for assisting these parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for others uses specifically required by law.
- 12.8.3 Business continuity in the event of a major disruption, disaster or failure.
- 12.8.4 Audit provisions that ensure that Payment Card Industry representative, or a Payment Card Industry approved third party, will be provided with full cooperation and access to conduct a thorough security review after a security intrusion. The review will validate compliance with the Payment Card Industry Data Security Standard for protecting cardholder data.
- 12.8.5 Termination provision that ensures that 3rd party will continue to treat cardholder data as confidential.

12.9 Implement an incident response plan

- **12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.**
- 12.9.1 Create an incident response plan to be used in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (e.g., informing Acquirers and credit card associations.).
- 12.9.2 Test the plan at least annually.
- 12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.
- 12.9.4 Provide appropriate training to staff with security breach response responsibilities.
- 12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
- 12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

Course summary

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Requirement 1: Install and maintain a firewall configuration to protect data

Requirement 5: Use and regularly update anti-virus software

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored data

Requirement 7: Restrict access to data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 6: Develop and maintain secure systems and applications

Requirement 9: Restrict physical access to cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

Congratulations

You have successfully completed the course

PCI-DSS 1.1 and associated Payment Card Industry controls

Unified Compliance Framework

Non-Compliance

Consequences

- Acquiring Banks
  - Financial institutions that grant retailers and other entities the approval needed to accept credit cards
    - Contractually responsible for ensuring merchant members comply
    - Determine merchant level
      - $5000 per instance per month for Mid Sized Merchant
      - $25000 per instance per month for Larger Merchants
      - Loss of the ability to take credit cards
  - Verisign report on 9/17/07 – Nearly 2/3s compliant

Incidents

TJ Max

- WEP compromise
- Minimum 18 month break in
- Affected 98 million credit card numbers
- Violated 9 of the 12 PCI requirements
- Fined $880,000 by Visa

Hannaford Brothers Grocery

- Company claimed PCI compliance in 02/08
- Timeline
  - Happened Dec. 7, 2007
  - Discovered Feb. 27, 2008
  - Contained March 10, 2008
- Exposed 4.2 million credit / debit card numbers
- 1800 credit / debit numbers stolen
- Inside job
- Sniffed while cards were processed

Challenges

Challenges

- Know data flow
- Scoping
- POS systems as apply to Requirement 5 and 6
  - *Requirement 5:* Use and regularly update anti-virus software
  - *Requirement 6:* Develop and maintain secure systems and applications
- Cost
  - Implementation (installing / maintaining)
  - Firewalls and Anti-Virus
- Data ownership – encrypting of stored data at rest
- Testing and Maintaining
  - Annual rotation of encryption keys
- Securing Applications
  - Minimizing amount of data stores
- Logging and protecting data

Possible Solutions

Possible Solutions

- Report any incidents to Visa or other brand
  - Breaches
  - Even if not sure – let the brand determine
- Limit the scope
  - Know where data is
  - Know where data is stored
  - Verify encryption
  - Reduce these areas
- Use certified applications and hardware for POS
- Know what level required to be compliant with
  - Acquirer makes this determination

Possible Solution (con't)

- If doing self-assessment, try to have third party verify
- Have a change management process
    - Know how changes affect the compliance
- Have Incident Response plan
    - Include Visa, Acquirer
    - Know regulations
        - State
        - Federal
        - Other
- Keep up with PCI changes
    - Check PCI SSC Website periodically
    - https://www.pcisecuritystandards.org/
- Quickly remediate issues

Payment Application Data Security Standard (PA-DSS)

PA-DSS

- Based on Visa Payment Application Best Practices (PABP)
- Approved April 2008
- Derived from PCI-DSS and PCI-DSS Security Audit Procedure
- Applies
  - Payment application typically sold and installed “Off the Shelf” without much customization
  - Payment application provided in modules
- Not Applied
  - Payment application developed for and sold to only one customer
    - Would be part of PCI-DSS compliancy
- Typical applications that are not Payment Application
  - Operating systems that PA is installed on (Windows, Linux)
  - Database systems that store cardholder data (Oracle, SQL)
  - Back office systems that store cardholder data (reporting)

PA-DSS (con't)

- Scope
    - Application functionality
    - End to end payment function (authorization and settlement)
    - Input / output
    - Error conditions
    - Interfaces and connections to other file systems, etc.
    - All cardholder data flow
    - Encryption mechanisms
    - Authentication mechanisms

PA-DSS (con't)

- Content for report a validation
  - Description of scope review
  - Executive Summary
  - Findings / Observation
  - Contact information and report date
- Audit Areas
  1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or pin block
  2. Protect stored cardholder data

PA-DSS (con't)

3. Provide secure authentication features
4. Log payment application activity
5. Develop secure payment applications
6. Protect wireless transmission
7. Test payment applications to address vulnerabilities
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote software update
11. Facilitate secure remote access to payment application
12. Encrypt all non-console administrative access
13. Encrypt sensitive traffic over public network
14. Maintain instruction documentation and training programs for customers, resellers, and integrators

PA-DSS (con't)

- Applicability to Hardware Terminals
  - Called dumb POS terminals or standalone POS terminals
  - No PA-DSS if ALL apply:
    - Terminal has no connection to any of the merchant's systems or network
    - Connects only to the acquirer or processor
    - Payment applications vendor provides Secure Remote
      - Updates
      - Troubleshooting
      - Access
      - Maintenance
  - Following never stored after authorization
    - Full contents of any track from the magnetic strip
    - Card-validation code or value
    - PIN or encrypted PIN Block

PA-DSS (con’t) - Roles

- Vendors
  - Developers of payment applications that store, process or transmit cardholder data as part of authorization or settlement and then sell distribute, or license these applications to third parties (customer, reseller / integrator)
- Customers
  - Merchant service providers or others who buy or receive a third party application to store, process, or transmit cardholder data as part of authorization or selling of payment transactions

PS-DSS (con’t) - Roles

- Resellers and Integrators
  - Sell, install and/or service payment applications on behalf of software vendors or others
- Payment Card Industry Security Standards Committee (PCI SSC)
  - Standards body that maintains PCI standards
  - www.pcisecuritystandards.org
- Payment Brands
  - American Express, Discover, JCB, Mastercard, Visa
  - Develop and enforce any program related to PA-DSS

QSA, ASV, PA-QSA

Qualified Security Assessors (QSA)

- Contracted directly with PCI SSC
- Only QSA can determine compliance
- Instituted for consistent and proper application of security measures and controls
- Qualifications requirements are exacting and detailed
- Both company and employee must be certified
- Process
  - Apply as a firm for qualification in the program
  - Provide document adhering to the Validation Requirements for Qualified Security Assessors
  - Qualify individual employees, though training and testing, to perform assessments
  - Execute an agreement with PCI SSC governing performance
- Renew yearly
- High costs

Approved Scanning Vendor (ASV)

- Validate compliance
- Perform a rigorous remote test on the PCI SSC test infrastructure, which simulates a typical customer
- Deliberate introduce vulnerabilities and misconfigurations for the vendor to identify and report as part of the compliance testing process
- Primary test addresses:
  - Scan administration – how the vendor collects and manages scan requests from its customers
  - Scan performance – the ability of each vendor to identify vulnerabilities and misconfigurations in the network and web applications
  - Scan report – how the vendor presents the scan results to its customers
- Subject to annual recertification
- Costly

Payment Application Qualified Security Assessor (PA-QSA)

- Must be employed by QSA company
- Must utilize the testing procedure documentation in PA-DSS document
- Must assess to laboratory where validation process
  - Simulates real world use of the payment application
- Follow requirements for the laboratory and laboratory processes
- Must complete and submit Appendix B in PA-DSS document completed for payment application under review as part of completed PA-DSS report

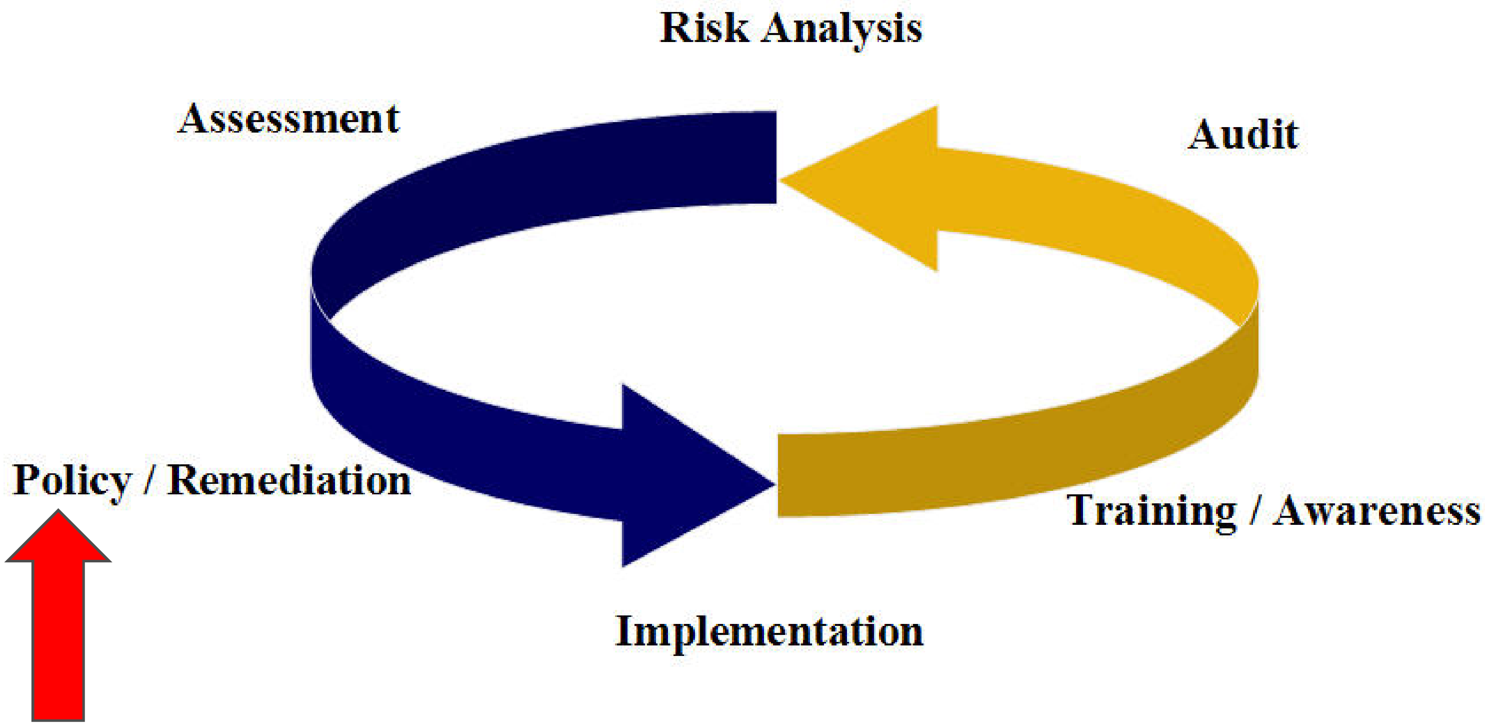
Bonus

Documenting Your Policies and Procedures

Discussion

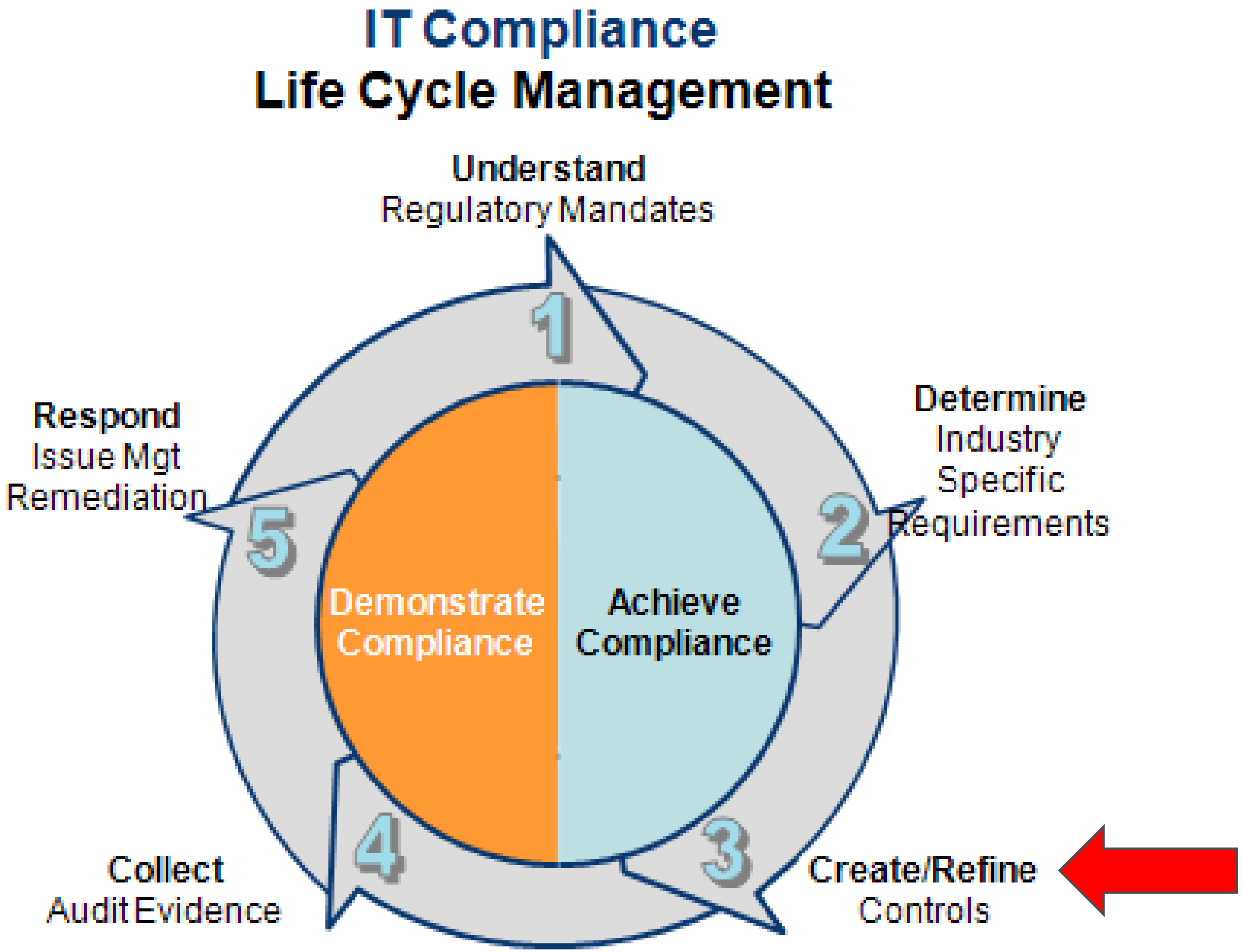
- Security Life Cycle
- Compliance Life Cycle
- What is a Policy
  - Why is it Needed
  - What is Required
- Policy Section Descriptions
- Policies to Consider
- Documenting Procedures
- Approval Process
- Validation Process
- Other Relevant Documents
- References

Security Life Cycle



From: Network Security – A Beginners Guide by Eric Maiwald

Compliance Life Cycle



What Is A Policy

- Webster Definition:

A definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions.

- UCF:

Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.

What Does A Policy Do

- Addresses A Business Need
- To Get By In Involve Other Departments Such as Legal, HR, Business Units
- States Who the Policy Applies To
- States What The Policy Is
- States Why The Policy Is Needed
- Be Concise
- Easy to Understand
- Easy to Read

Describes The Organization's Decision to Enact a Control or Set of Controls

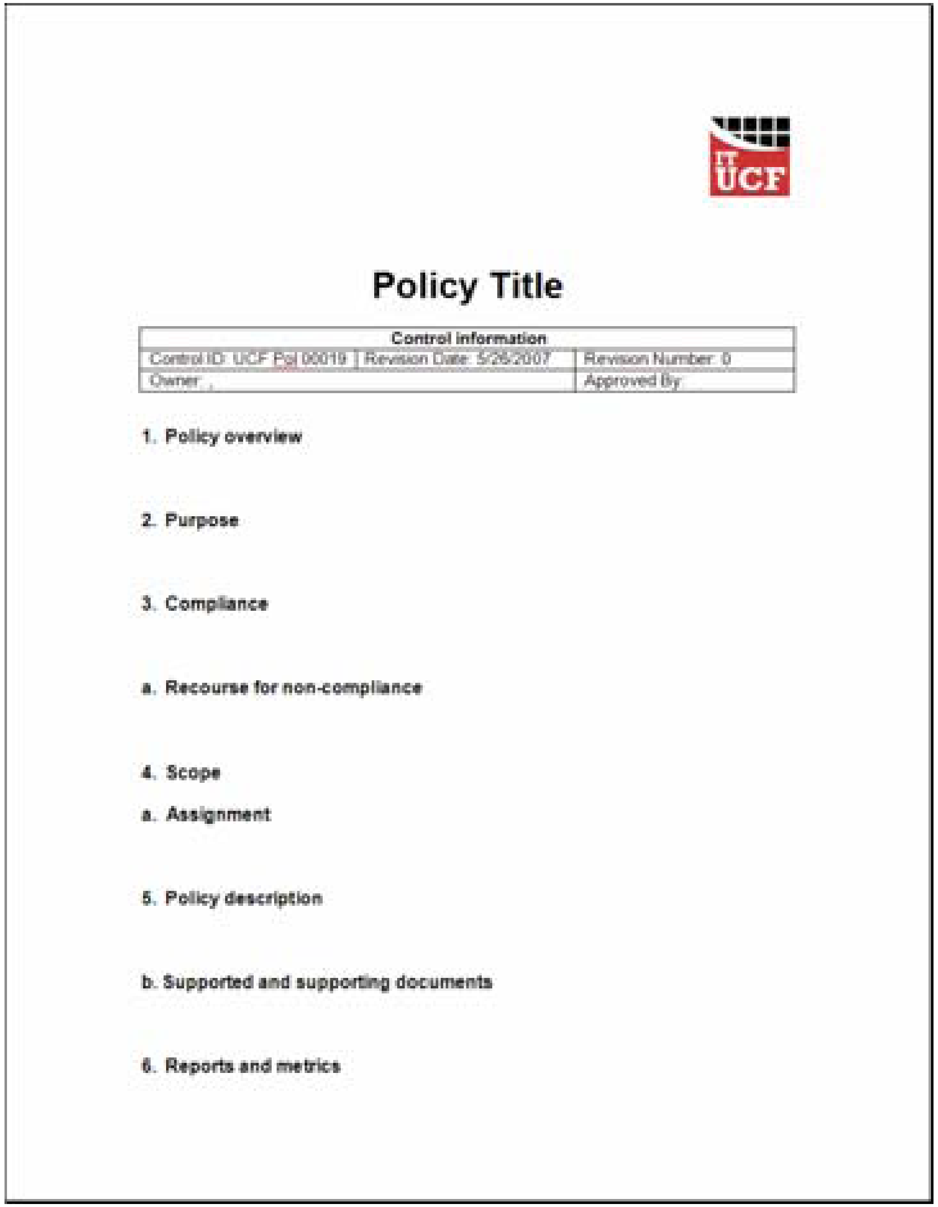
Why Is Policy Needed

- To show employees most appropriate way to behave
- Guidance in handling various situations
- When needed to protect the company legally
- To keep company in compliance with regulations and laws
- Establish consistent work standards, rules and regulations
- Provide consistent and fair treatment for all employees

What Is Required In A Policy

- Title
- ID
- Effective Date
- Guarantor or Approver
- Policy Overview
- Purpose
- Compliance With Public and Organizational Rules
- Consequences of Non-Compliance
- Scope
- Description (Policy) Extended Definition (Procedure)
- Reports or Metrics

Policy Format Example 1



Policy Title

Control information		
Control ID: UCF Pol 00019	Revision Date: 5/26/2007	Revision Number: 0
Owner:		Approved By:

1. Policy overview

2. Purpose

3. Compliance

a. Recourse for non-compliance

4. Scope

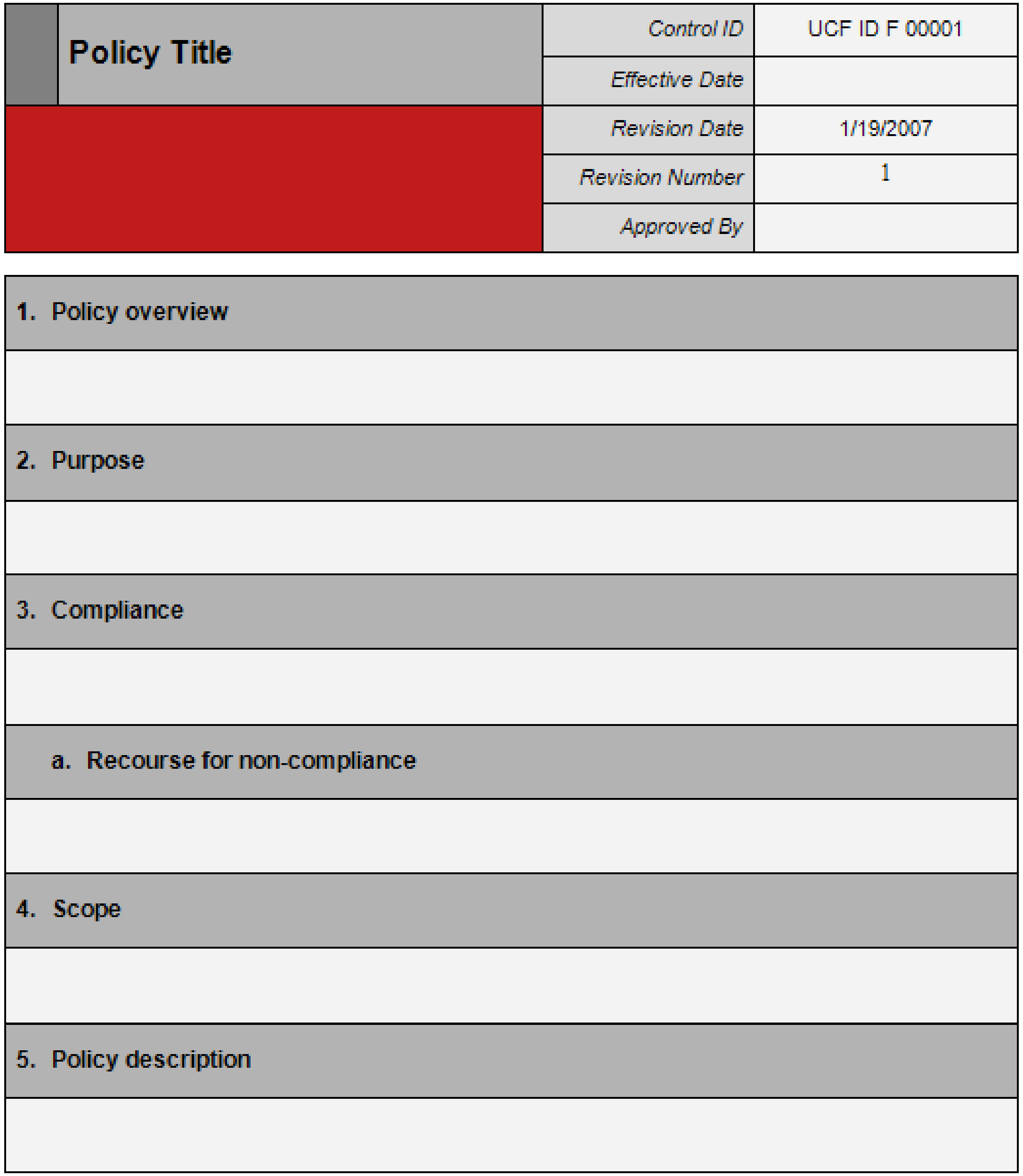
a. Assignment

5. Policy description

b. Supported and supporting documents

6. Reports and metrics

Policy Format Example 2



Policy Title	*Control ID*	UCF ID F 00001
	Effective Date	
	Revision Date	1/19/2007
	Revision Number	1
	Approved By	

1. Policy overview

2. Purpose

3. Compliance

   a. Recourse for non-compliance

4. Scope

5. Policy description

Policy Section Descriptions

- Policy Identification Information
  - Discerns One Policy from the Next
- Title
  - Unique Name for Policy
  - Ex. Password Policy
- ID
  - Should be Unique
  - Ex. UCF 01111
- Effective Date
  - Date Policy is Approved and Completed

Policy Section Description (con’t)

- Revision Number
  - Always Start with 1.0
  - Should Be Entered Automatically if Possible
  - Use Version Tracking for Creating and Editing Policies
- Guarantor or Approver
  - Person approving or accepting the policy
  - This Approval Puts The Policy in Effect and Enforceable

Policy Section Descriptions (con’t)

- Policy Overview
  - Heart of Whole Policy
  - Reflect Tone of Organization in It’s Direction and Meaning
  - Does Not Have To Be Long, but Short and to the Point
  - When Written for Compliance Can Be Taken From Regulation, Standard, etc.
  - UCF Consists of Policy Statements
- Overview Example:

The organization will ensure that the continuity plan addresses considerations and continuity solutions for websites (extranet, intranet, workflow) and coordinates those solutions with all relevant support groups

Policy Section Descriptions (con't)

- Purpose
  - Defines the Goal That Needs to be Achieved
  - Concise
  - Comprehensive
  - A Couple of Sentences
  - Tells Reader Why Policy Must be Followed
- Purpose Statement Example:

The purpose of the policy is to ensure that the websites have been properly documented for configuration changes to the hardware and the software and any configurable items have been catalogued and accounted for in the continuity plan. The coordination steps are necessary to ensure proper integration with both security plans and incident management plans.

Policy Section Descriptions (con’t)

- Importance of “Why” Statement
  - Most People Will Not Follow Unless They Know WHY They are being Told to Follow it and it’s Impact
  - Makes Policy Easier to Understand and Justifies it to the Reader
  - Help Support Regulatory Requirements for Awareness and Training
  - Demonstrates Business Need and Makes Clear it was Not Just Created by IT Security
  - Clarifies Interpretation Giving User Guidance When Faced With Gray Areas

Policy Section Descriptions (con’t)

- Compliance
  - Citations of Authority Documents
  - Validation of Policy
- Consequences of Non-Compliance
  - Steps Taken to Enforce Policy
  - Could be it’s Own Global Policy, thus Optional in Most Policies
  - Prevents Policy Circumvention and Users Ignoring Policy
  - Involve HR and Possibly Legal

Policy Section Descriptions (con't)

- Scope
  - Tells Who the Policy Applies to
- Policy Description
  - Two General Types of Policy
    - Issue-Specific
      - Developed to Address Particular Activities or Systems
      - Condensed Procedural Steps
      - Read in Under 60 Seconds
      - Don't Get to Techno
      - One-to-One Relationship Between Controls and Policies

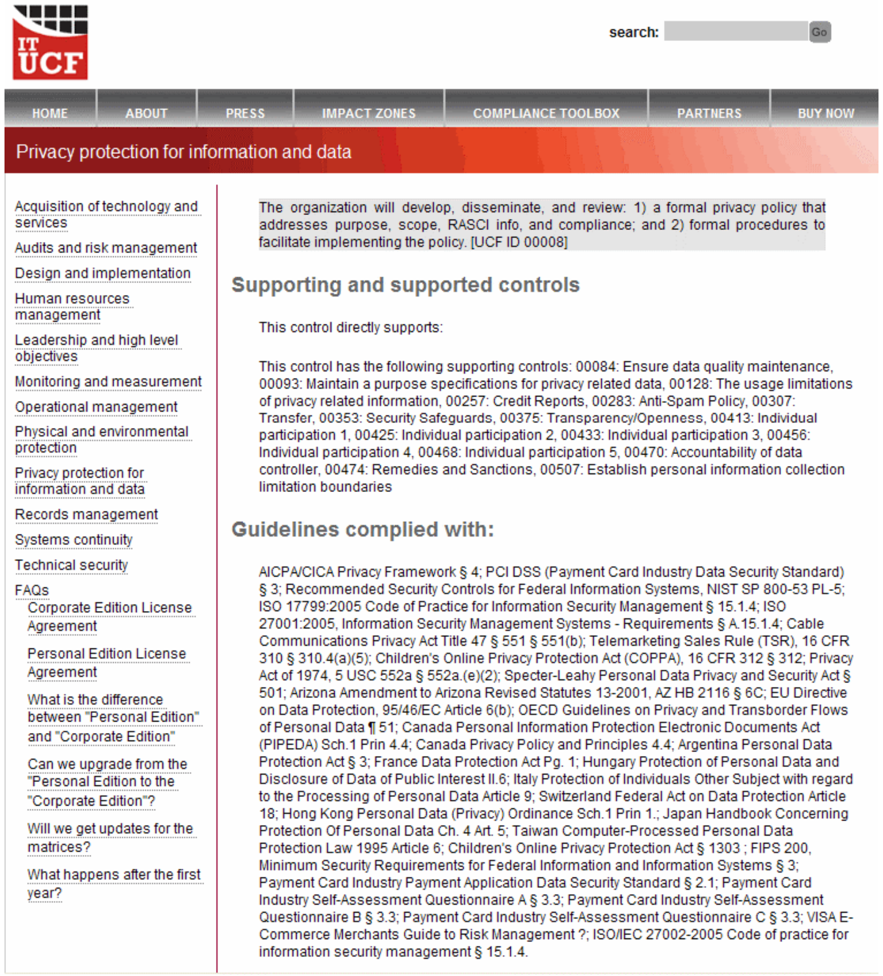
Policy Section Descriptions (con't)

- Types of Policy (con't)
  - Program-Level
    - Used to Write for a Grouped Set of Controls
    - Longer than Normal Statement
    - Will Be Divided Into Several Procedures
    - Primary Purpose
      - Document Organization-Wide Goals
      - Define Program Management Structure
      - Define Reporting Responsibilities
      - Clarify Roles and Responsibilities Across a Set of Multiple Controls

Policy Section Descriptions (con’t)

- Reports and Metrics
  - Reporting and Metrics States How You are Going to Measure Whether or Not the Policy is being Followed.
  - Within the UCF Metrics Have Been Predefined and You can Align Policies with the Specific Metrics that Match the Policy Type.

UCF Control


IT UCF
search:
Go
HOME
ABOUT
PRESS
IMPACT ZONES
COMPLIANCE TOOLBOX
PARTNERS
BUY NOW

Privacy protection for information and data

Acquisition of technology and services
Audits and risk management
Design and implementation
Human resources management
Leadership and high level objectives
Monitoring and measurement
Operational management
Physical and environmental protection
Privacy protection for information and data
Records management
Systems continuity
Technical security
FAQs
Corporate Edition License Agreement
Personal Edition License Agreement
What is the difference between "Personal Edition" and "Corporate Edition"
Can we upgrade from the "Personal Edition to the "Corporate Edition"?
Will we get updates for the matrices?
What happens after the first year?

The organization will develop, disseminate, and review: 1) a formal privacy policy that addresses purpose, scope, RASCI info, and compliance; and 2) formal procedures to facilitate implementing the policy. [UCF ID 00008]

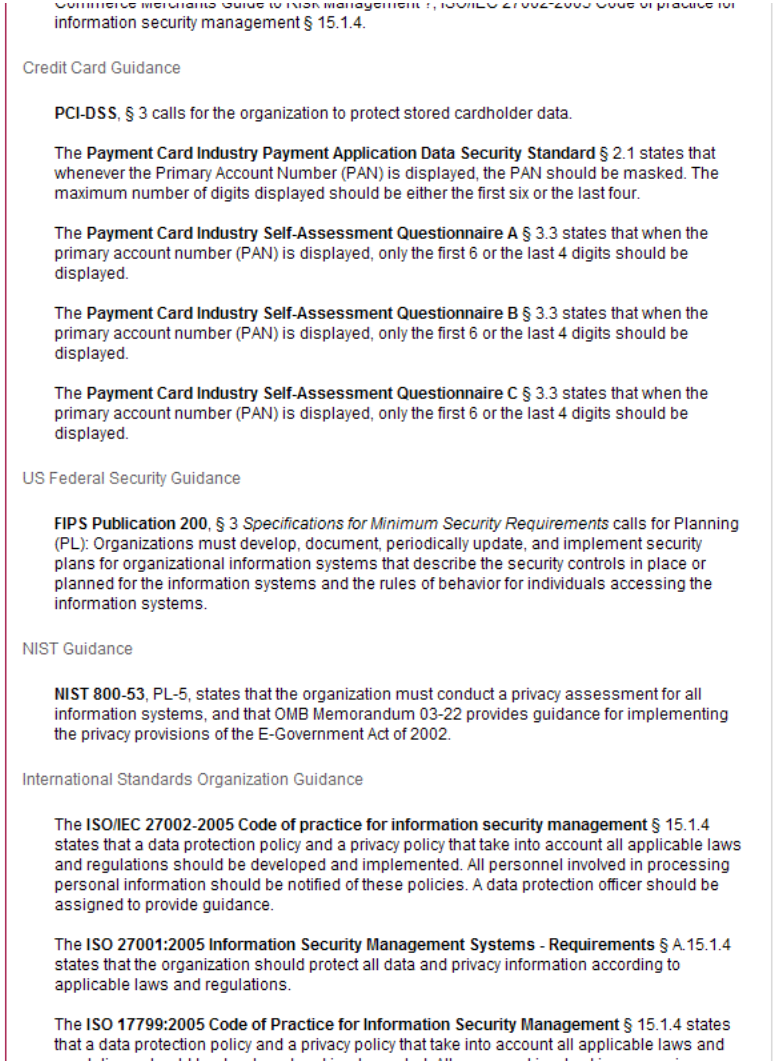
Supporting and supported controls

This control directly supports:

This control has the following supporting controls: 00084: Ensure data quality maintenance, 00093: Maintain a purpose specifications for privacy related data, 00128: The usage limitations of privacy related information, 00257: Credit Reports, 00283: Anti-Spam Policy, 00307: Transfer, 00353: Security Safeguards, 00375: Transparency/Openness, 00413: Individual participation 1, 00425: Individual participation 2, 00433: Individual participation 3, 00456: Individual participation 4, 00468: Individual participation 5, 00470: Accountability of data controller, 00474: Remedies and Sanctions, 00507: Establish personal information collection limitation boundaries

Guidelines complied with:

AICPA/CICA Privacy Framework § 4; PCI DSS (Payment Card Industry Data Security Standard) § 3; Recommended Security Controls for Federal Information Systems, NIST SP 800-53 PL-5; ISO 17799:2005 Code of Practice for Information Security Management § 15.1.4; ISO 27001:2005, Information Security Management Systems - Requirements § A.15.1.4; Cable Communications Privacy Act Title 47 § 551 § 551(b); Telemarketing Sales Rule (TSR), 16 CFR 310 § 310.4(a)(5); Children's Online Privacy Protection Act (COPPA), 16 CFR 312 § 312; Privacy Act of 1974, 5 USC 552a § 552a.(e)(2); Specter-Leahy Personal Data Privacy and Security Act § 501; Arizona Amendment to Arizona Revised Statutes 13-2001, AZ HB 2116 § 6C; EU Directive on Data Protection, 95/46/EC Article 6(b); OECD Guidelines on Privacy and Transborder Flows of Personal Data ¶ 51; Canada Personal Information Protection Electronic Documents Act (PIPEDA) Sch.1 Prin 4.4; Canada Privacy Policy and Principles 4.4; Argentina Personal Data Protection Act § 3; France Data Protection Act Pg. 1; Hungary Protection of Personal Data and Disclosure of Data of Public Interest II.6; Italy Protection of Individuals Other Subject with regard to the Processing of Personal Data Article 9; Switzerland Federal Act on Data Protection Article 18; Hong Kong Personal Data (Privacy) Ordinance Sch.1 Prin 1.; Japan Handbook Concerning Protection Of Personal Data Ch. 4 Art. 5; Taiwan Computer-Processed Personal Data Protection Law 1995 Article 6; Children's Online Privacy Protection Act § 1303 ; FIPS 200, Minimum Security Requirements for Federal Information and Information Systems § 3; Payment Card Industry Payment Application Data Security Standard § 2.1; Payment Card Industry Self-Assessment Questionnaire A § 3.3; Payment Card Industry Self-Assessment Questionnaire B § 3.3; Payment Card Industry Self-Assessment Questionnaire C § 3.3; VISA E-Commerce Merchants Guide to Risk Management ?; ISO/IEC 27002-2005 Code of practice for information security management § 15.1.4.



Commerce Merchants Guide to Risk Management ?; ISO/IEC 27002-2005 Code of practice for information security management § 15.1.4.

Credit Card Guidance

PCI-DSS, § 3 calls for the organization to protect stored cardholder data.

The **Payment Card Industry Payment Application Data Security Standard** § 2.1 states that whenever the Primary Account Number (PAN) is displayed, the PAN should be masked. The maximum number of digits displayed should be either the first six or the last four.

The **Payment Card Industry Self-Assessment Questionnaire A** § 3.3 states that when the primary account number (PAN) is displayed, only the first 6 or the last 4 digits should be displayed.

The **Payment Card Industry Self-Assessment Questionnaire B** § 3.3 states that when the primary account number (PAN) is displayed, only the first 6 or the last 4 digits should be displayed.

The **Payment Card Industry Self-Assessment Questionnaire C** § 3.3 states that when the primary account number (PAN) is displayed, only the first 6 or the last 4 digits should be displayed.

US Federal Security Guidance

FIPS Publication 200, § 3 *Specifications for Minimum Security Requirements* calls for Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

NIST Guidance

NIST 800-53, PL-5, states that the organization must conduct a privacy assessment for all information systems, and that OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

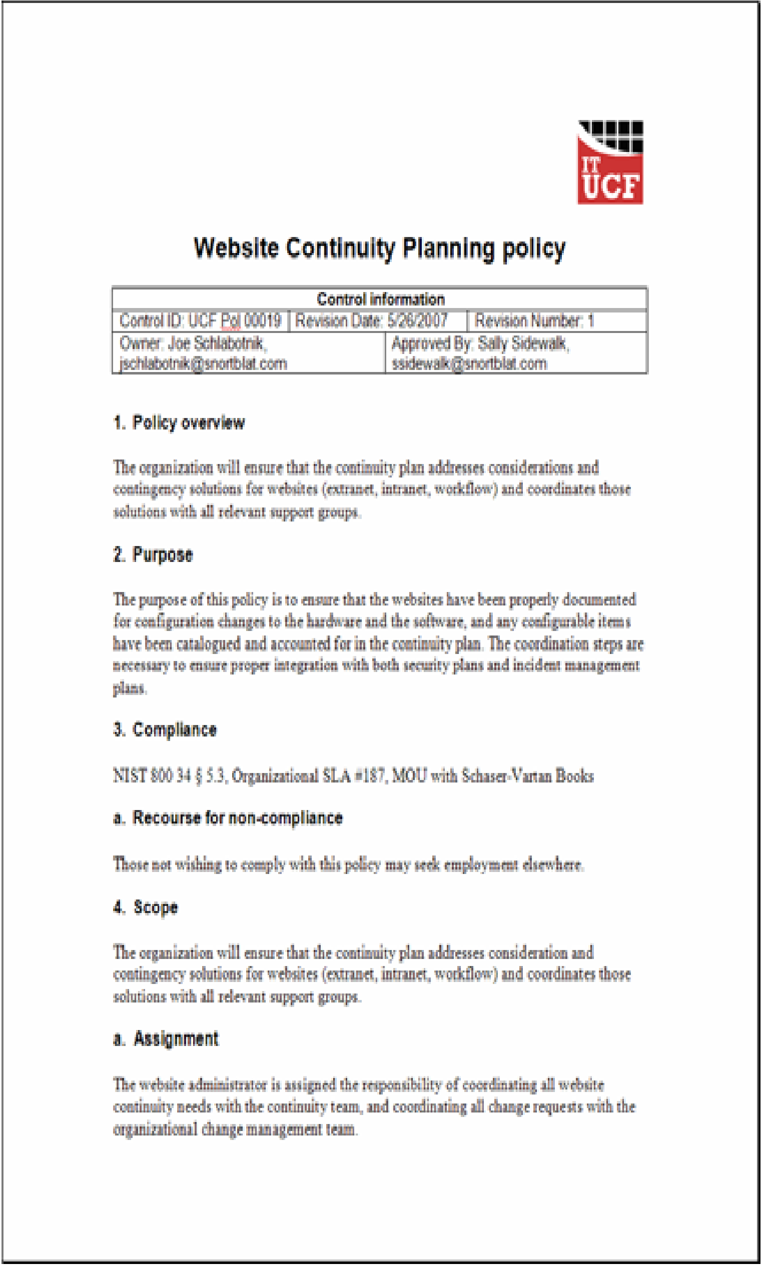
International Standards Organization Guidance

The **ISO/IEC 27002-2005 Code of practice for information security management** § 15.1.4 states that a data protection policy and a privacy policy that take into account all applicable laws and regulations should be developed and implemented. All personnel involved in processing personal information should be notified of these policies. A data protection officer should be assigned to provide guidance.

The **ISO 27001:2005 Information Security Management Systems - Requirements** § A.15.1.4 states that the organization should protect all data and privacy information according to applicable laws and regulations.

The **ISO 17799:2005 Code of Practice for Information Security Management** § 15.1.4 states that a data protection policy and a privacy policy that take into account all applicable laws and

Completed Policy Example



Website Continuity Planning policy

Control information		
Control ID: UCF Pol 00019	Revision Date: 5/26/2007	Revision Number: 1
Owner: Joe Schlabotnik, jschlabotnik@snortblat.com	Approved By: Sally Sidewalk, ssidewalk@snortblat.com	

1. Policy overview

The organization will ensure that the continuity plan addresses considerations and contingency solutions for websites (extranet, intranet, workflow) and coordinates those solutions with all relevant support groups.

2. Purpose

The purpose of this policy is to ensure that the websites have been properly documented for configuration changes to the hardware and the software, and any configurable items have been catalogued and accounted for in the continuity plan. The coordination steps are necessary to ensure proper integration with both security plans and incident management plans.

3. Compliance

NIST 800 34 § 5.3, Organizational SLA #187, MOU with Schaser-Vartan Books

a. Recourse for non-compliance

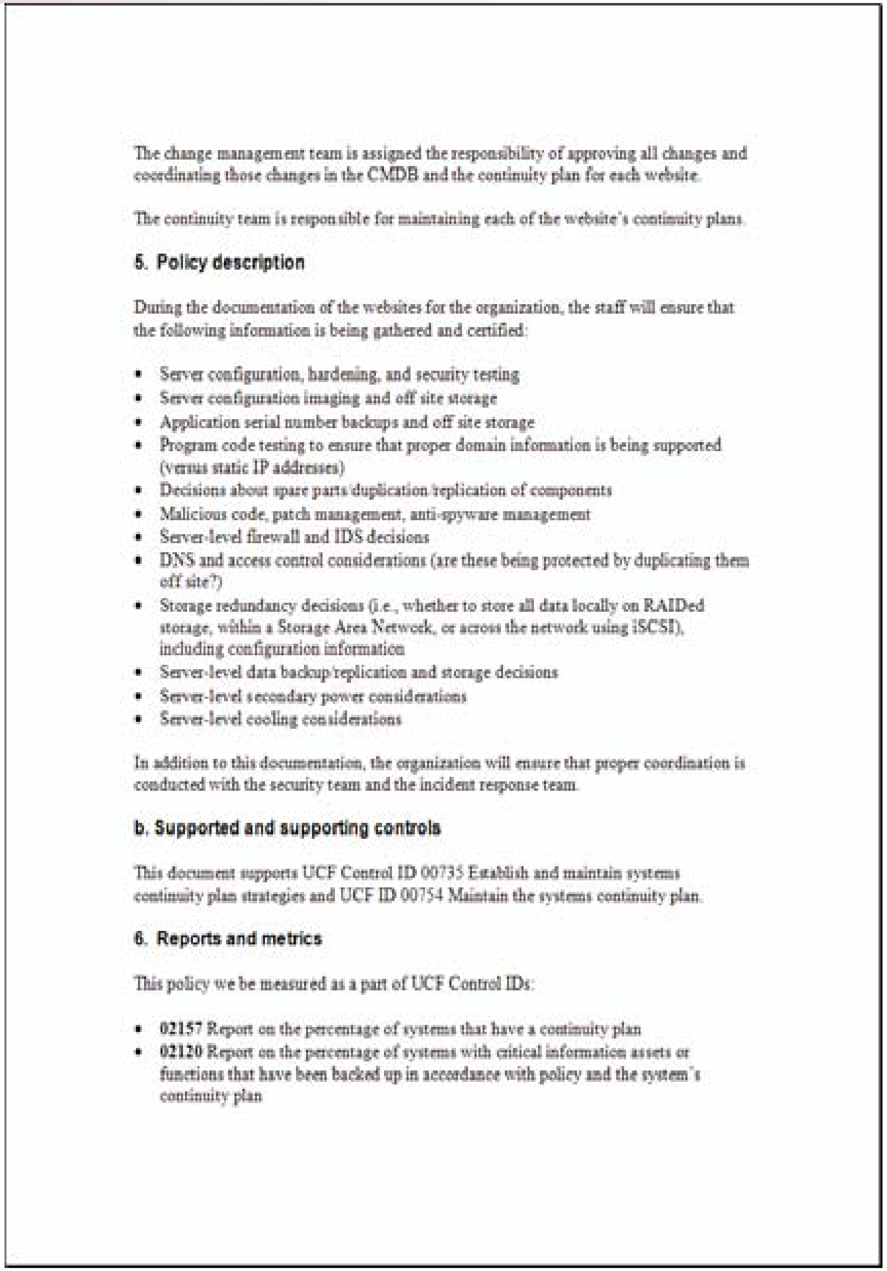
Those not wishing to comply with this policy may seek employment elsewhere.

4. Scope

The organization will ensure that the continuity plan addresses consideration and contingency solutions for websites (extranet, intranet, workflow) and coordinates those solutions with all relevant support groups.

a. Assignment

The website administrator is assigned the responsibility of coordinating all website continuity needs with the continuity team, and coordinating all change requests with the organizational change management team.



The change management team is assigned the responsibility of approving all changes and coordinating those changes in the CMDB and the continuity plan for each website.

The continuity team is responsible for maintaining each of the website's continuity plans.

5. Policy description

During the documentation of the websites for the organization, the staff will ensure that the following information is being gathered and certified:

- Server configuration, hardening, and security testing
- Server configuration imaging and off site storage
- Application serial number backups and off site storage
- Program code testing to ensure that proper domain information is being supported (versus static IP addresses)
- Decisions about spare parts/duplication/replication of components
- Malicious code, patch management, anti-spyware management
- Server-level firewall and IDS decisions
- DNS and access control considerations (are these being protected by duplicating them off site?)
- Storage redundancy decisions (i.e., whether to store all data locally on RAIDed storage, within a Storage Area Network, or across the network using iSCSI), including configuration information
- Server-level data backup/replication and storage decisions
- Server-level secondary power considerations
- Server-level cooling considerations

In addition to this documentation, the organization will ensure that proper coordination is conducted with the security team and the incident response team.

b. Supported and supporting controls

This document supports UCF Control ID 00735 Establish and maintain systems continuity plan strategies and UCF ID 00754 Maintain the systems continuity plan.

6. Reports and metrics

This policy we be measured as a part of UCF Control IDs:

- **02157** Report on the percentage of systems that have a continuity plan
- **02120** Report on the percentage of systems with critical information assets or functions that have been backed up in accordance with policy and the system's continuity plan

General Policies That You May Consider

- Acceptable Use
- Anti-Virus / Anti-Malware
- Change Control
- Encryption
- Access Control
  - Physical
  - Employees (Role Based)
  - Vendors
  - Partners
  - Remote
  - Visitors
- Media Handling
- Secure Coding

- Security Policy / Plan
- Policy Review / Update
- Incident Response
- Disaster Recovery / BC
- Data Retention/Disposition
- Data Classification
- Labeling
- Responsibilites
- Key Management
- Password / ID
- Email
- Training / Awareness
- Configuration Control

Documenting Procedures

- Scope
  - Who is being Affected
  - What is being Affected
- Coverage
  - Which System(s), Network(s), Application(s), and Personnel Does Control Apply
  - Identify All people and IT Assets Affected
- Assignment
  - Documented According to RACI Model
  - Responsibility Accountable Consulted Informed
  - One Person with Authority for Step
  - One Person with Responsibility for Step

RACI Assignment Chart

R = Responsible A = Accountable **C = Consulted I = Informed**	Server Admin	Code Mgr	DBA	IT Security	CIRT	LOB Mgr	Client Contact	DR Mgr	IT Director
Document server hardware and software configurations	R		C			C	C		A
Document configuration imaging management	C		C					R	A
Document application serial number backups	C							R	A
Document records backup procedures	C		C					R	A
Document spare part & storage redundancy decisions	C							R	A
Document system hardening configurations	C			R					A
Document system security configurations	C			R					A
Test application programming techniques for security and access control		R		C			I		A
Document access control (including domain issues) configurations	C			R			I		A
Document system cooling and secondary power configurations	R								A
Document system configurations with incident management	C				R				A

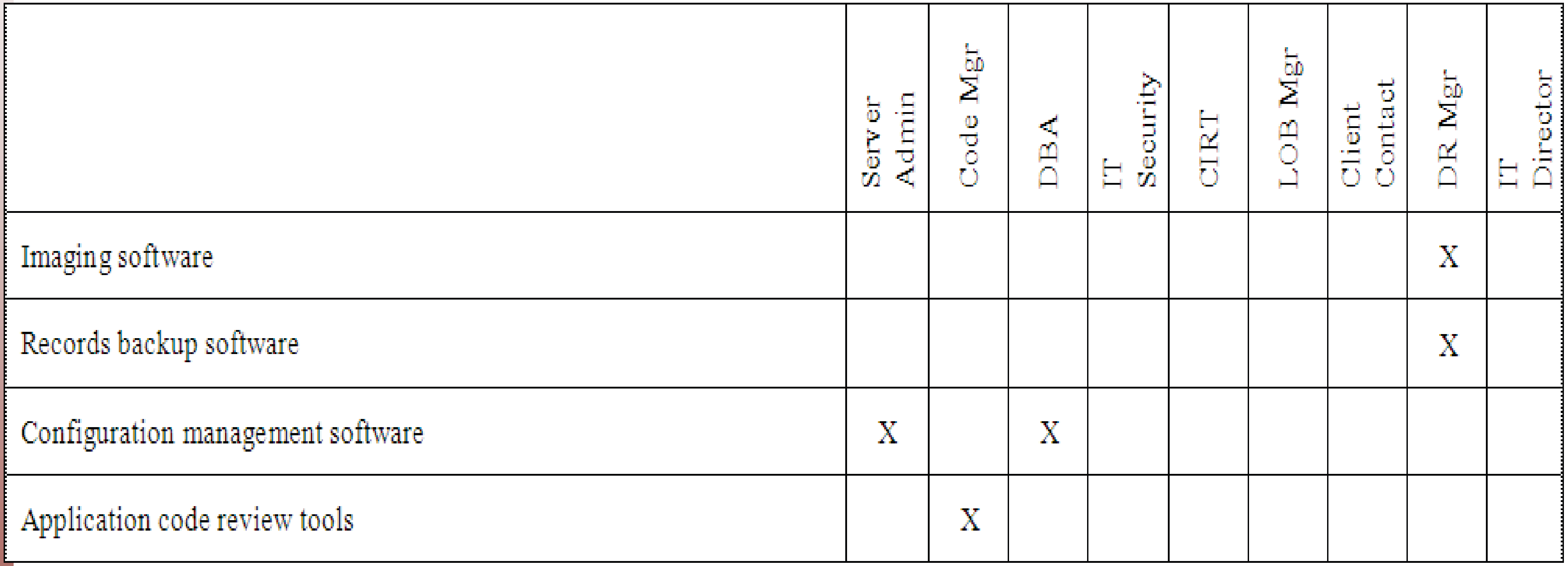
Documenting Procedures (con't)

- Required Knowledge
  - What Information is Needed to Carry Out Control
  - Training or Certification Needed to Perform Control
- Required Tools
  - Necessary Tools Individuals or Roles Needed to Complete Assigned Procedure

Team Knowledge Chart

	Server Admin	Code Mgr	DBA	IT Security	CIRT	LOB Mgr	Client Contact	DR Mgr	IT Director
Use of organizational system documentation template	X	X	X	X	X	X		X	X
Use of imaging software								X	
Use of records backup software								X	
Database Management system			X						
Storage management hardware and software	X		X						
Knowledge of system hardening methodology	X			X					X
Application code review skills		X							
Domain Naming schema for the organization	X	X	X	X	X			X	X
System security plans	X			X	X				X
Incident management procedures	X				X				X
Systems Continuity planning and documentation	X							X	X

Team Tools Chart



	Server Admin	Code Mgr	DBA	IT Security	CIRT	LOB Mgr	Client Contact	DR Mgr	IT Director
Imaging software								X	
Records backup software								X	
Configuration management software	X		X						
Application code review tools		X							

Documenting Procedures (con't)

- Extended Definition
  - Provides Additional Information
    - Goals
    - Triggers
    - Other Information That May Be Needed
- Procedure Goals
  - More In-depth than Policy Statement
  - Create Overall Summary of Policy Description
- Supporting and Supported Procedures
  - List Procedures that Current One Supports
  - List Procedures that Support Current One

Documenting Procedures (con't)

- Procedure Triggers
  - Indicate When the Procedure Should be Run
  - Minimum – Annually for Testing
    - Indicate any Exceptions and Who has the Authority to Run This Procedure
- Potential Mishaps & Reaction Steps
  - Use Chart to Show Symptom, Possible Causes, Solution
- Successful Execution
  - List of Items That Show the Success of the Process
- Reports
  - All Documents Showing Complete and Success of Procedure

Documenting Potential Mishaps

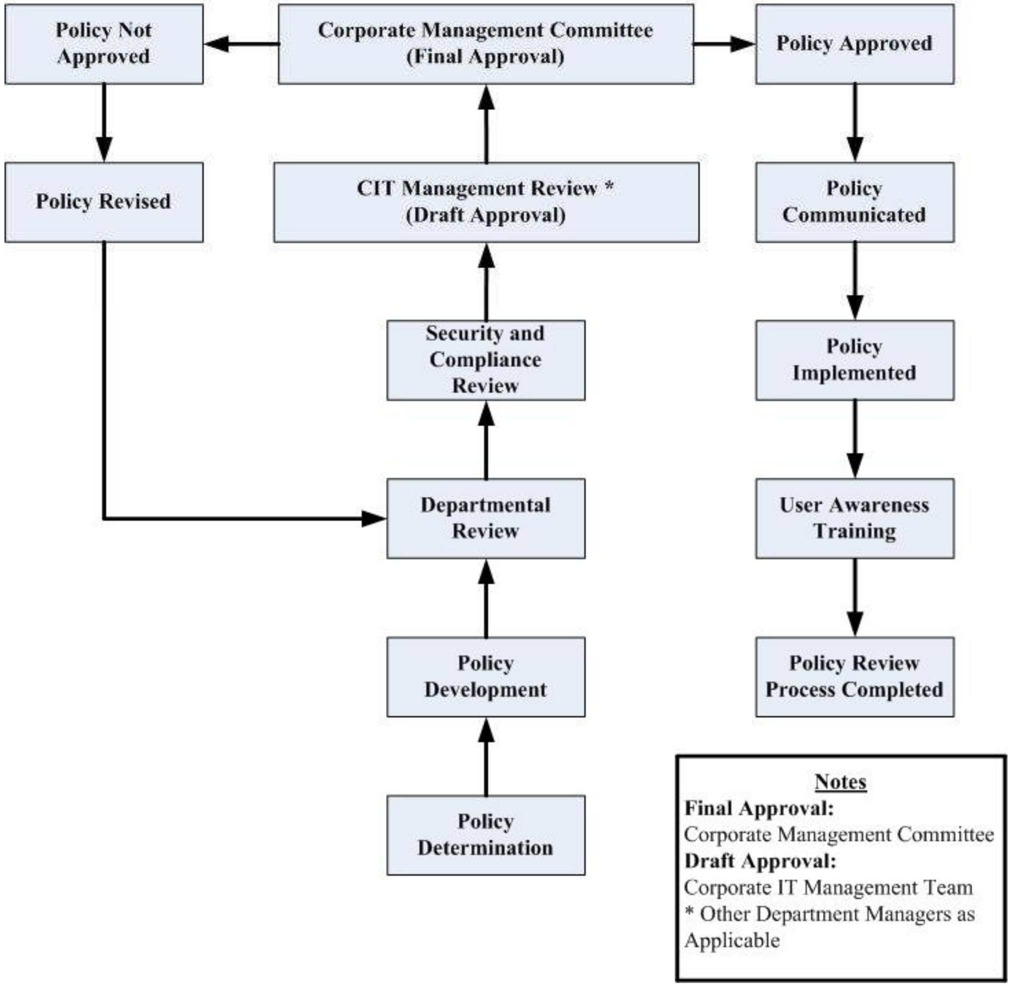
Analyze website hardware & software configurations		
Symptom	Possible Cause	Solution
Can't access configuration programs	Invalid AD rights	Check with AD admin for proper rights and account information
	Are you using the right software?	Check the prior configuration documentation for the configuration application's version number and compare that to the one you are using. If incorrect, re-install the configuration management application from the application library.
	Have you checked the password?	If you are having password problems, call the AD admin and have the password reset.
Analyze website application programming		
Symptom	Possible Cause	Solution
The server's software is live and in production	The test load data set is not set to live	Call the DB Admin and have the test load data set brought to "on line" status for testing.

Documenting Procedures (con't)

- Procedure Steps
  - Simple Outline
  - Flow Charts
  - Screen Shots
  - Digital Pictures
  - Textual Reference
  - System Forms
  - Hardware / Software Configuration
- Procedure Checklist
  - Provide Clues on What Should be On Hand Before Beginning the Procedure
    - Tools
    - People
- Detailed Revision History
  - Same as Policy

Review and Approval Process Example

Policy Approval Process Example



Notes

Final Approval:
Corporate Management Committee
Draft Approval:
Corporate IT Management Team
* Other Department Managers as Applicable

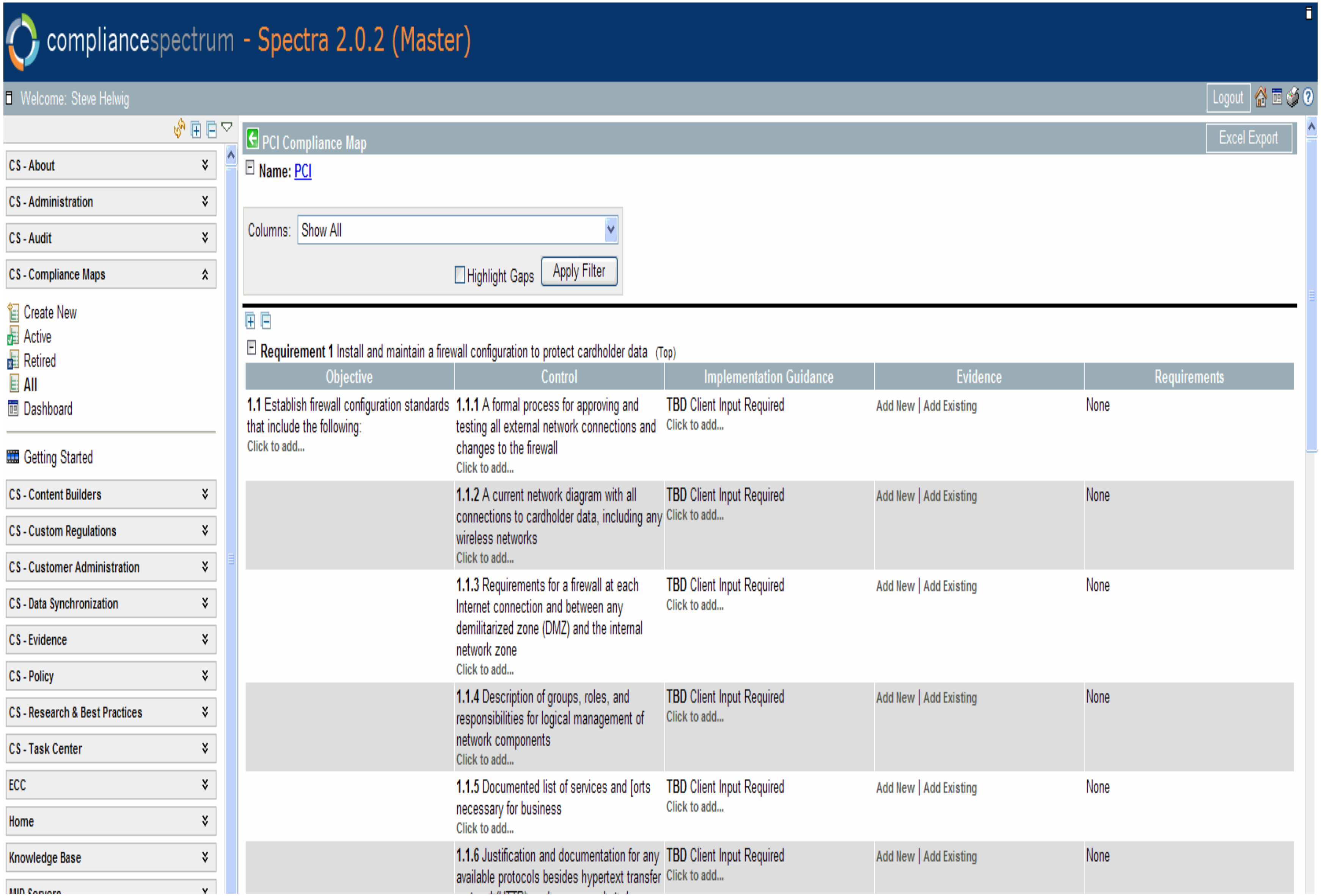
Validation Process Questions

- Questions to Ask Subject Matter Experts When Validating Policy and Procedures
  - Does the Policy or Procedure Links Directly to a Control as Defined in Control Framework List?
  - Is This a Policy or a Procedure?
    - States Who, What, and Why – Policy
    - States How - Procedure
  - Is the Policy or Procedure Valid – Can be Accomplished?
  - Does the Final Policy and/or Procedure Compare Equally to the Original Draft and Annotated Change Notes?
  - Does the Math Work?
    - Ensure Correctness of any Numbers, Calculations, Etc.
  - Are There Any Additional Mishaps that Should be Considered?
  - Does the Procedure Come to a Different Conclusion or “Success” Point than Documented?
  - Does the Procedure Require the Reader to Exercise Discretion or Good Judgment?

Other Relevant Documents

- Network Diagrams
- Organization Charts
- Data Flow Diagrams
- Asset Management
- System, Network, Etc. Configurations
- System, Network, Change Documents

Where Does It Fit



Name: PCI

Columns: Show All

☐ Highlight Gaps

Requirement 1 Install and maintain a firewall configuration to protect cardholder data (Top)

Objective	Control	Implementation Guidance	Evidence	Requirements
1.1 Establish firewall configuration standards that include the following: Click to add...	1.1.1 A formal process for approving and testing all external network connections and changes to the firewall Click to add...	TBD Client Input Required Click to add...	Add New | Add Existing	None
	1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks Click to add...	TBD Client Input Required Click to add...	Add New | Add Existing	None
	1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone Click to add...	TBD Client Input Required Click to add...	Add New | Add Existing	None
	1.1.4 Description of groups, roles, and responsibilities for logical management of network components Click to add...	TBD Client Input Required Click to add...	Add New | Add Existing	None
	1.1.5 Documented list of services and [orts necessary for business Click to add...	TBD Client Input Required Click to add...	Add New | Add Existing	None
	1.1.6 Justification and documentation for any available protocols besides hypertext transfer	TBD Client Input Required Click to add...	Add New | Add Existing	None

References

The Compliance Authority:

http://www.thecomplianceauthority.com/

IT UCF:

http://www.thecomplianceauthority.com/unifiedcompliance.shtml

http://www.unifiedcompliance.com/

Say What You Do:…

http://www.unifiedcompliance.com/it_compliance/say_what_you_do/

Compliance Glossary

http://www.unifiedcompliance.com/it_compliance/language_compliance/

Change Management Toolkit

http://www.unifiedcompliance.com/it_compliance/change_management/products/the_change_management_toolkit.html

Systems and Information Classification

http://www.unifiedcompliance.com/it_compliance/systems_info_class/

PCI SSC:

www.pcisecuritystandards.org

Conclusion

Q & A

Thanks for Attending