

UNRAVELLING THE MYSTERIES OF THE PCI-DSS STANDARDS

And make your organizations compliant

Ralph Villanueva PCI-ISA PCIP CISA CISM ITIL CIA
CRMA CFE CPA (Phil) MBA

IT Security and Compliance Analyst

Diamond Resorts International

NCPACA & PASCAPA 32nd Annual Professional Convention 2018

Objectives

- Provide an overview of the PCI-DSS standards
- Explain the importance of complying with the PCI-DSS standards
- Point out how accounting and finance professionals can help make their organizations compliant

About Ralph Villanueva

- IT compliance professional since 2010
- Payment Card Industry – Internal Security Assessor (PCI-ISA), Payment Card Industry Professional (PCIP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), IT Infrastructure Library (ITIL), Certified Internal Auditor (CIA), Certification in Risk Management Assurance (CRMA), Certified Fraud Examiner (CFE) and CPA (Phil)
- BSBA from UPV and MBA from Ateneo de Manila University
- Believes that Filipino accounting professionals are among the best in the world

POLLING QUESTION

1. How many of you use at least one credit or debit card?
2. How many of you work for organizations that accept credit or debit cards?

Why is the PCI-DSS important?

NCPACA & PASCAPA 32nd Annual Professional Convention 2018

Why this is important to you?

- Savings for your organization - less audit fees paid if you can do some of the work
- Better appreciation of interconnectedness of all controls – more meaningful recommendations
- IKAW AY MAGIGING SIKAT – Your career will get a substantial boost, you're more likely to get that promotion, that salary increase and even your boss' daughter (if you're single)

Why you can do it?

- Similar to accounting, more work, less pay
- Compare accounting entry to GAAP
- Compare IT observation to IT compliance framework
- Prepare report of observations, impact and recommendations



What is PCI-SSC?

The PCI SSC is an independent industry standards body providing oversight of the development and management of Payment Card Industry Data Security Standards on a global basis.

The PCI SSC provides training for several different qualifications and programs.

PCI SSC founding payment brands include:

- American Express
- Discover Financial
- JCB International
- MasterCard
- Visa, Inc.



What is PCI-DSS

Payment Card Industry – Data Security Standards

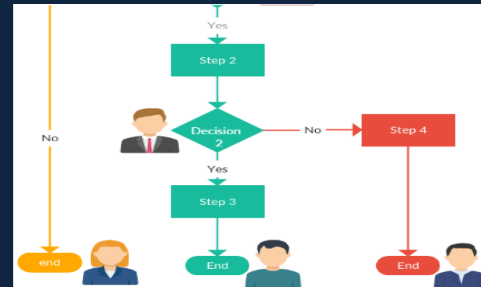
- Systems that store, process or transmit card holder data
- Systems that provide security services or may impact security of cardholder data environment (CDE)
- Any other component or device located within or connected to the CDE

PCI-DSS covers

- People



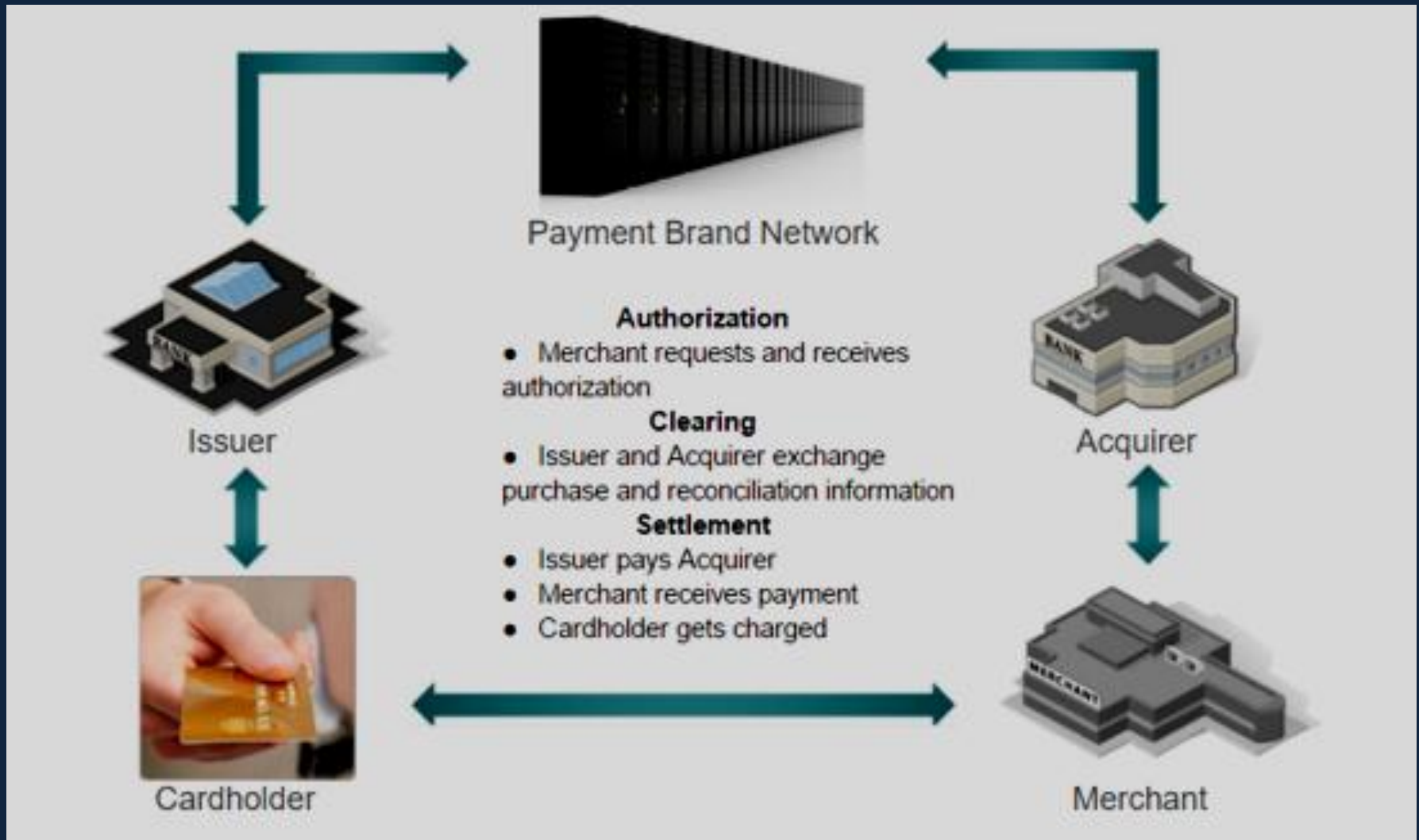
- Process



- Technology



Parties to a payment card transaction



Six main categories

- Build and maintain a secure network and systems
- Protect card holder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Twelve requirements

PCI Data Security Standard – High Level Overview

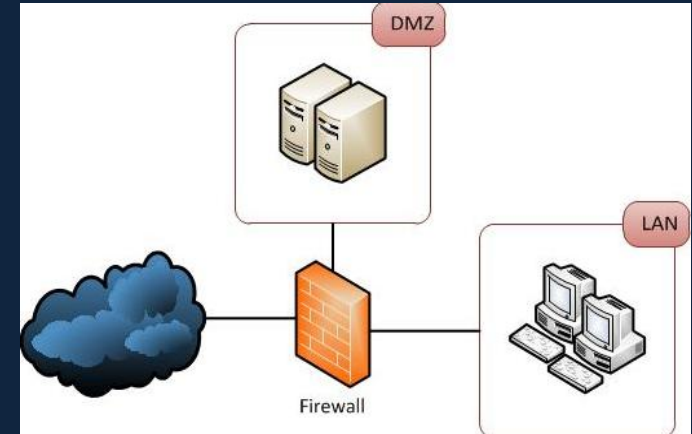
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Protect all systems against malware and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel

How can you help your organization be compliant?

- Leverage your position within the organization as trusted and competent management advisers
- Communicate the PCI-DSS requirements to everyone who processes, stores and transmits card holder data
- Be familiar with the PCI-DSS requirements

Requirement#01: Install and maintain a firewall configuration to protect card holder data

- Latest software version and updated patches
- Implicit deny all
- Access control list
- Reviewed every six months
- Security policies & operational procedures for managing firewalls are documented, in use and known to all affected parties



Requirement#02:Do not use vendor-supplied defaults for system passwords and other security parameters

- Shoulder surf with your IT admins
- No default passwords
- Encrypted non-console access
- Security policies & operational procedures for managing vendor defaults are documented, in use and known to all affected parties

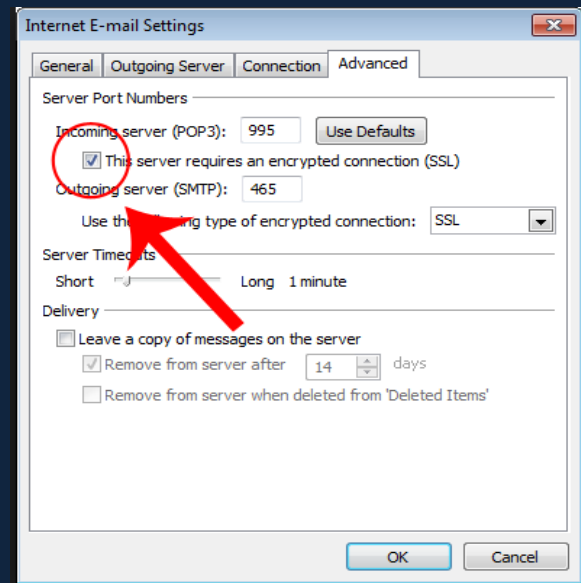
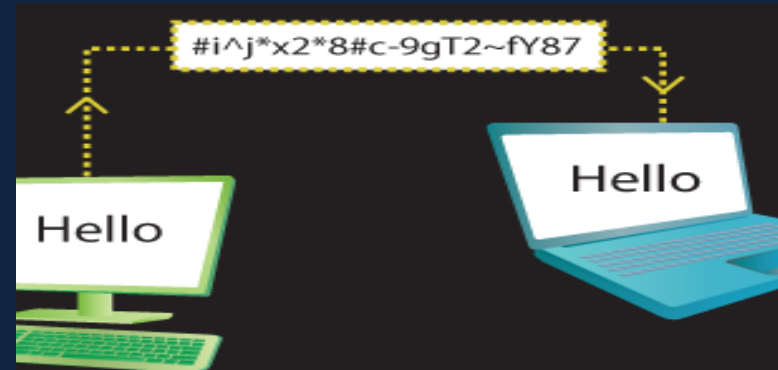
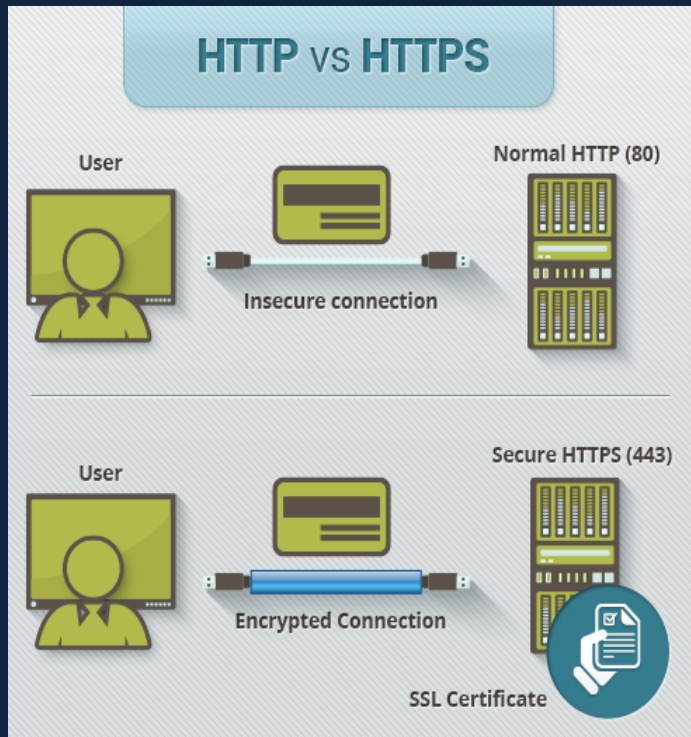
Linksys		
Model	Default Username	Default Password
WAP11	n/a	(none)
DSL	n/a	admin
EtherFast Cable/DSL Router	Administrator	admin
Linksys Router DSL/Cable	(none)	admin
BEFW11S4 1	admin	(none)
BEFSR41 2	(none)	admin
WRT54G	admin	admin
WAG54G	admin	admin
ap 1120	n/a	(none)
Linksys DSL	n/a	admin
WAP54G 2	(none)	admin

Requirement#03: Protect stored card holder data

- Encryption
- Data retention and disposal policies and procedures
- Mask card account number when displayed
- Security policies & operational procedures for protecting stored card holder data are documented, in use and known to all affected parties



Requirement#04: Encrypt transmission of cardholder data across open public networks



Requirement#05: Protect all systems against malware and regularly update anti-virus systems and programs

- Latest version and patches
- Deployed to all computers susceptible to malware
- Users cannot be admins; cannot disable anti-virus
- Security policies & operational procedures for protecting systems against malware are documented, in use and known to all affected parties

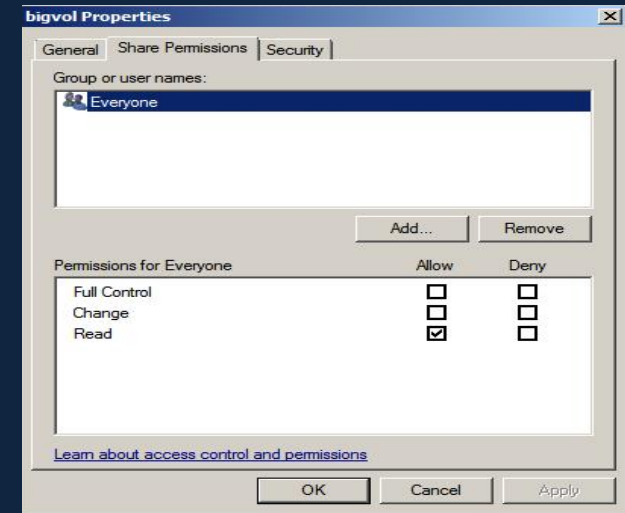


Requirement#06: Develop and maintain secure systems and applications

- Security vulnerability analysis & risk ranking
- Incorporate information security during development
- Change control processes
- Segregation of duties between development & production teams
- Functionality testing and back-out procedures
- Security policies & operational procedures for developing secure systems and applications are documented, in use & known to all affected parties

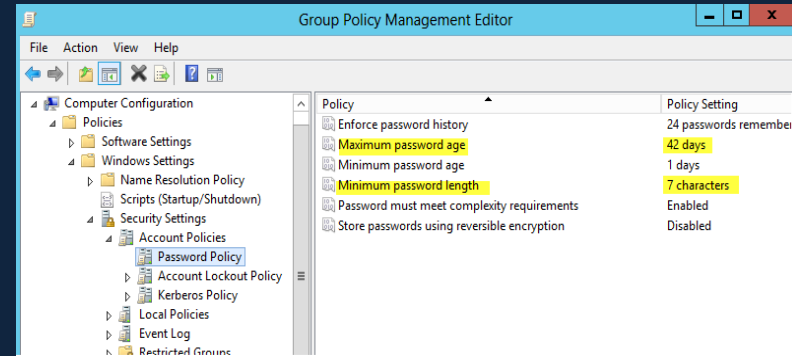
Requirement#07: Restrict access to card holder data by business need to know

- Least privilege
- Access after management approval
- Access based on job classification & function
- Security policies & operational procedures for restricting access to cardholder data are documented, in use & known to all affected parties



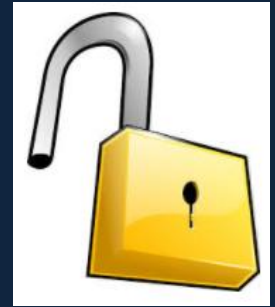
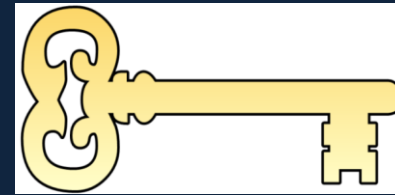
Requirement#08: Identify and authenticate access to system components

- Unique user names and passwords
- Password at least 7 alpha, numeric and special characters, change every 90 days
- Lockout after 6 attempts
- Multi factor non-console access
- Security policies & operational procedures to identify and authenticate are documented, in use and known to all affected parties



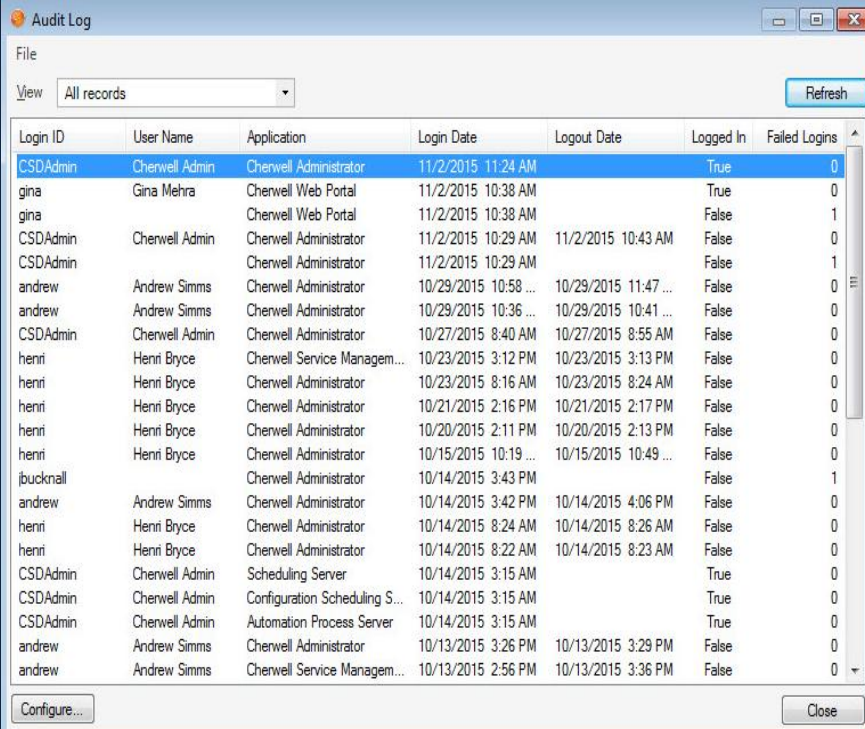
Requirement#09: Restrict physical access to card holder data

- Facility entry controls
- Restrict physical access to wireless access points, network and telecom equipment
- Control physical access to sensitive areas and strict control over storage and access to media
- Updated list of computers
- Inspect devices to detect tampering
- Policies & procedures documented, in use & known to all



Requirement#10: Track and monitor all access to network resources and card holder data

- Computer activity logs & audit trails
- Invalid logical access
- Changes to system – level objects
- Someone reviews logs & security events
- Retention of audit trails for one year, with 3 months ready for analysis
- Policies & operational procedures documented, in use and known to all affected parties



The screenshot shows a window titled "Audit Log" with a menu bar (File) and a "View" dropdown set to "All records". A "Refresh" button is in the top right. The main area is a table with the following columns: Login ID, User Name, Application, Login Date, Logout Date, Logged In, and Failed Logins. The table contains 20 rows of log entries.

Login ID	User Name	Application	Login Date	Logout Date	Logged In	Failed Logins
CSDAdmin	Cherwell Admin	Cherwell Administrator	11/2/2015 11:24 AM		True	0
gina	Gina Mehra	Cherwell Web Portal	11/2/2015 10:38 AM		True	0
gina	Gina Mehra	Cherwell Web Portal	11/2/2015 10:38 AM		False	1
CSDAdmin	Cherwell Admin	Cherwell Administrator	11/2/2015 10:29 AM	11/2/2015 10:43 AM	False	0
CSDAdmin	Cherwell Admin	Cherwell Administrator	11/2/2015 10:29 AM		False	1
andrew	Andrew Simms	Cherwell Administrator	10/29/2015 10:58 ...	10/29/2015 11:47 ...	False	0
andrew	Andrew Simms	Cherwell Administrator	10/29/2015 10:36 ...	10/29/2015 10:41 ...	False	0
CSDAdmin	Cherwell Admin	Cherwell Administrator	10/27/2015 8:40 AM	10/27/2015 8:55 AM	False	0
henri	Henri Bryce	Cherwell Service Managem...	10/23/2015 3:12 PM	10/23/2015 3:13 PM	False	0
henri	Henri Bryce	Cherwell Administrator	10/23/2015 8:16 AM	10/23/2015 8:24 AM	False	0
henri	Henri Bryce	Cherwell Administrator	10/21/2015 2:16 PM	10/21/2015 2:17 PM	False	0
henri	Henri Bryce	Cherwell Administrator	10/20/2015 2:11 PM	10/20/2015 2:13 PM	False	0
henri	Henri Bryce	Cherwell Administrator	10/15/2015 10:19 ...	10/15/2015 10:49 ...	False	0
jucknall		Cherwell Administrator	10/14/2015 3:43 PM		False	1
andrew	Andrew Simms	Cherwell Administrator	10/14/2015 3:42 PM	10/14/2015 4:06 PM	False	0
henri	Henri Bryce	Cherwell Administrator	10/14/2015 8:24 AM	10/14/2015 8:26 AM	False	0
henri	Henri Bryce	Cherwell Administrator	10/14/2015 8:22 AM	10/14/2015 8:23 AM	False	0
CSDAdmin	Cherwell Admin	Scheduling Server	10/14/2015 3:15 AM		True	0
CSDAdmin	Cherwell Admin	Configuration Scheduling S...	10/14/2015 3:15 AM		True	0
CSDAdmin	Cherwell Admin	Automation Process Server	10/14/2015 3:15 AM		True	0
andrew	Andrew Simms	Cherwell Administrator	10/13/2015 3:26 PM	10/13/2015 3:29 PM	False	0
andrew	Andrew Simms	Cherwell Service Managem...	10/13/2015 2:56 PM	10/13/2015 3:36 PM	False	0

Requirement#11:Regularly test security systems and processes

- Incident response procedures
- Quarterly internal and external vulnerability scans
- Annual internal and external penetration tests
- Presence of intrusion detection and prevention systems
- Policies & operational procedures documented, in use & known to all affected parties

Requirement#12: Maintain a policy that addresses security for all personnel

- Establish, publish, maintain and disseminate a security policy
- Annual risk assessment process
- Inventory of critical technologies, owners and access
- Defined information security management responsibilities
- Formal security awareness program
- Employees to acknowledge annually security policy and procedures
- Screen employees prior to hire

Some aspects of IT security policies

- Acceptable Use Policy
- Information Security Awareness & Training
- BYOD Policy
- Data Storage Retention & Disposal Policy
- Data Classification Policy
- Internet Security Policy
- IT Security Roles Policy

Some tips on PCI-DSS compliance work

- N - Never stop pestering IT with answers
- C - Collaborate with stakeholders
- P - PCI-DSS
- A - Auditor mindset
- C - Consult with peers and industry contacts
- A - Attitude

Bonus round

- What is the happiest place on earth in California?
- Who founded Disneyland?
- What is the latest newly opened attraction? (Hint: Two words both starts with P)

Thank you

Here are some online resources

www.pcisecuritystandards.org

www.isaca.org

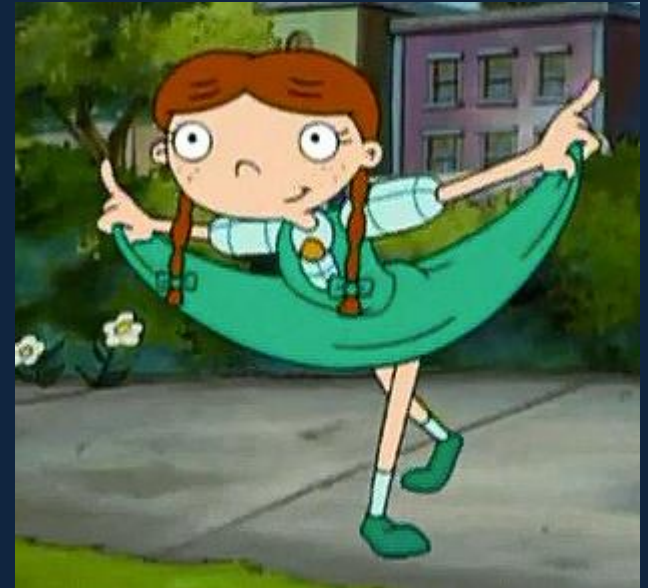
www.us-cert.gov

www.iapp.org

www.coso.org

For more info, my email is:

rvsvillanueva@yahoo.com



NCPACA & PASCAPA 32nd Annual Professional Convention 2018