

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

PCI Compliance

What Do Credit Unions Need to
Know?

June 2019



Create Opportunities
We promise to know you and help you.

CLA – A Professional Services Firm

- A professional services firm with three distinct business lines
 - Wealth Advisory
 - Outsourcing
 - Audit, Tax, and Consulting
- More than 6,500 professionals
- Offices coast to coast
- Serve more than 1,500 financial institutions



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.



Cyber Security Services

Information Security offered as specialized service offering for over 20 years

- Largest Credit Union Service Practice*
 - Penetration Testing and Vulnerability Assessment
 - Black Box, Red Team, and Collaborative Assessments
 - IT/Cyber security risk assessments
 - IT audit and compliance (GLBA, FFIECI, CIS, etc...)
 - **PCI-DSS Readiness and Compliance Assessments**
 - Incident response and forensics
 - Independent security consulting
 - Internal audit support
-
- **At last count... CLA was one of only 5 firms in the nation with all three of these designations/affiliations/capabilities**

*Callahan and Associates 2018 Guide to Credit Union CPA Auditors.



C:\whoami

- “Professional Student”
- Science Teacher/Self Taught Computer Guy
- IT Consultant - Project Manager – IT Staff/Help Desk - Hacker
- Assistant Scout Master (Boy Scouts)



2018 Breaches That Included Payment Cards



VISA

Newegg

Saks Fifth
Avenue

BevMo

Chili's

Panera

Applebee's

Peet's

Wellington
Online



Skimmers - examples



Skimmers - examples



Marketplace for Stolen Information

Attackers buy and sell data on cyber black market
– “The Dark Web” - similar to amazon.com

Home Buy CC CC Orders **Buy Dumps** Dump orders Checker Tickets Hello, [User] Cart (1) 9.45\$ Balance: 3.0\$ [Add money](#) [Replace policy](#) Logout

101 201

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#) [Clear](#) [Search](#)

	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	30\$	+
	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	30\$	+
	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	30\$	+
	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	30\$	+
	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	30\$	+
	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 95512, Olympia, WA	AMERICAN EXPRESS COMPANY	American Sanctions 14	30\$	+
	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	30\$	+
	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK Dump or cc of this particular bank (BIN)	American Sanctions 14	24\$	+



Exercise

- Normally a five minute exercise...
- Describe how your organization stores, processes, or transmits credit card information
- Think in terms of the steps/stages followed

Examples:

- ◊ Accept payment information over the phone
 - ◊ Members make payments online
 - ◊ Receive payment information in the mail
 - ◊ Member statements are sent/stored/reviewed by member services reps
-
- End goal is to understand “where the card data lives”



Exercise – QUESTIONS

- Do you accept CC payment “in-person”?
- Do you accept CC payment over the phone?
- Do you accept CC payment via a website?
- Do you rely on a 3rd party/vendor to host or manage any of your data systems?
- Do you store or process CC data for someone else?
- Do you have instant issue capabilities?
- Are ATM machines “on your network”?





PCI - DSS Overview

A Long Time Ago... In a Place Far Far Away...

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Overview – PCI DSS

Each major card brand had its own separate criteria for implementing credit card security.

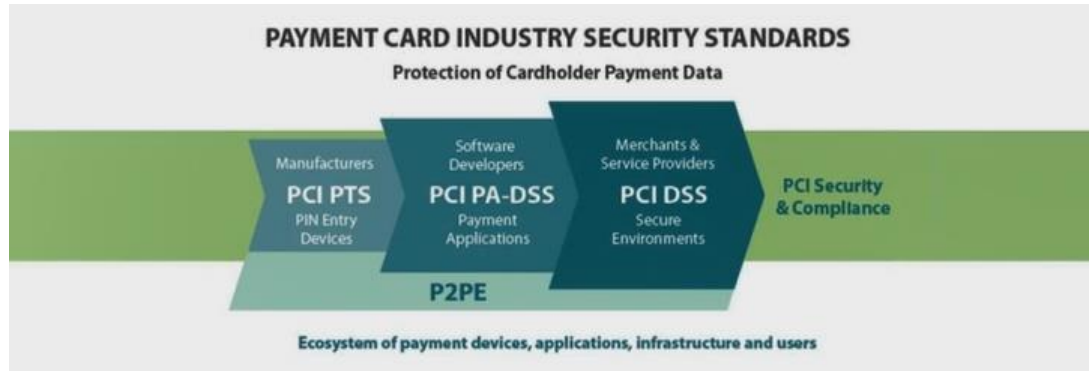
Merchants and processors who accepted multiple brands of cards needed to have a separate compliance program for each.

- Visa's Cardholder Information Security Program
- MasterCard's Site Data Protection
- American Express' Data Security Operating Policy
- Discover's Information Security and Compliance
- JCB's Data Security Program



The PCI Security Standards

- **In 2006**, the major payment card brands formed the Payment Card Industry Security Standards Council (PCISSC).
- This council developed and has continually updated the Data Security Standard (DSS) that all merchants must adhere to worldwide.
- The DSS is a set of 12 detailed requirements that ensure maximum payment card security.



PCI DSS Requirements

“The Digital Dozen”

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



Cardholder Data (CHD)

The PCI DSS defines CHD to be:

“At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.”

- **PAN** – Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account
- **Service Code** – Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
- **SAD** – Acronym for “sensitive authentication data.” Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.



Cardholder Data Environment (CDE)

The PCI DSS defines the CDE to be “*the people, processes and technology* that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.”

- **Store** – when cardholder data is inactive or at rest (e.g., located on electronic media, system component memory, paper, etc...)
- **Process** – when cardholder data is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed, etc...)
- **Transmit** – when cardholder data is being transferred from one location to another (e.g., data in motion)

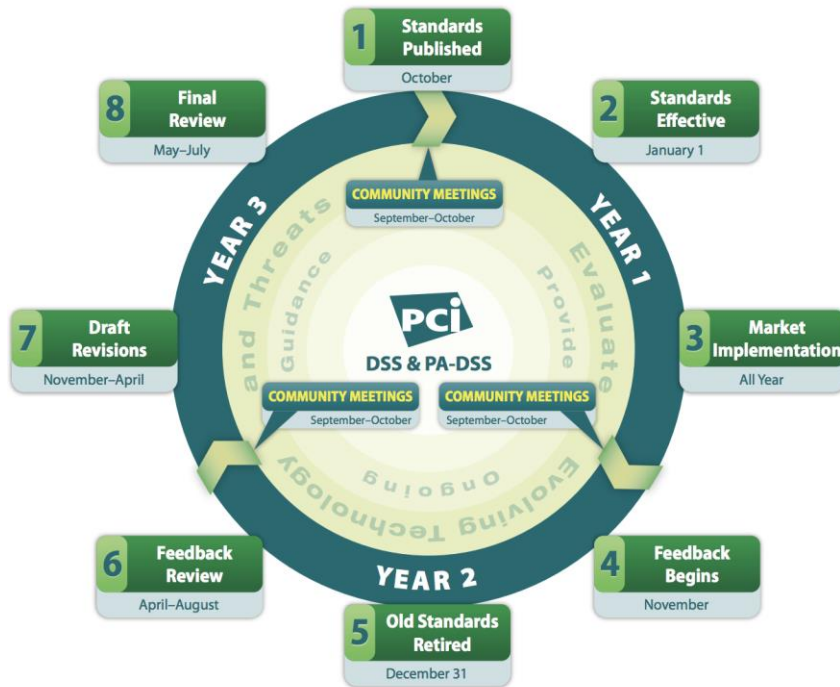


PCI DSS Timeline

- Version 1.0 – December 15, 2004
- Version 1.1 – September 6, 2006
- Version 1.2 - October 1, 2008
- Version 2.0 – October 2010
- Version 3.0 – November 2013
- Version 3.1 – April 2015
- Version 3.2 – April 2016
- Version 3.2.1 – May 2018

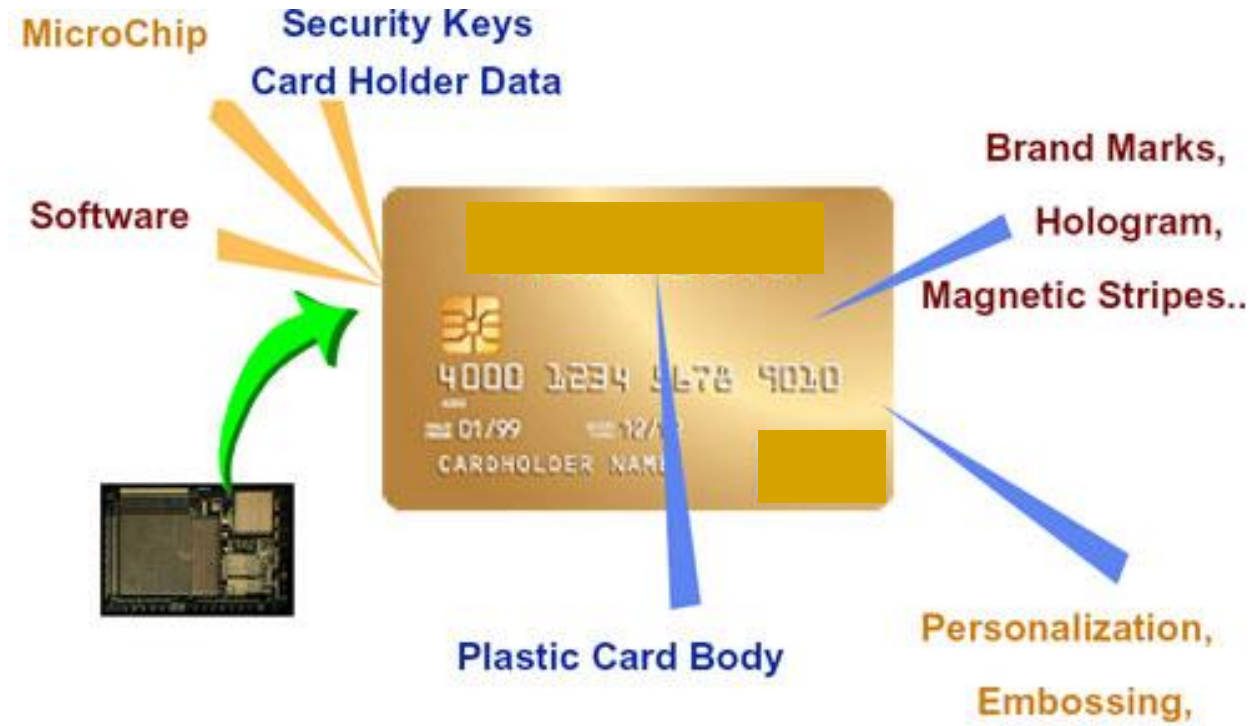


Lifecycle Changes to PCI DSS



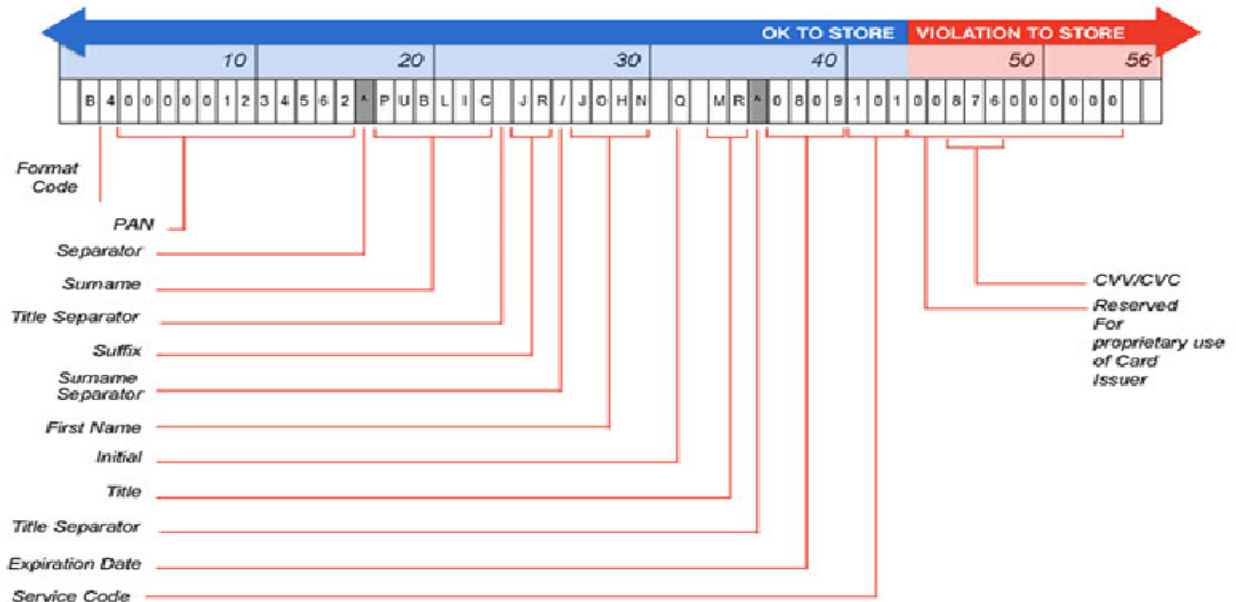
- https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

The Basics – Your Credit Card



The Basics – What is “Card Data”

Track 1 Data



The Basics – How Card Processing Works

Cardholder

- Consumers purchasing goods either as a “Card Present” or “Card Not Present” transaction
- Receives the payment card and bills from the issuer

Issuer

- Bank or other organization issuing a payment card on behalf of a Payment Brand (e.g. MasterCard & Visa)
- Payment Brand issuing a payment card directly (e.g. Amex, Discover, JCB)

Merchant

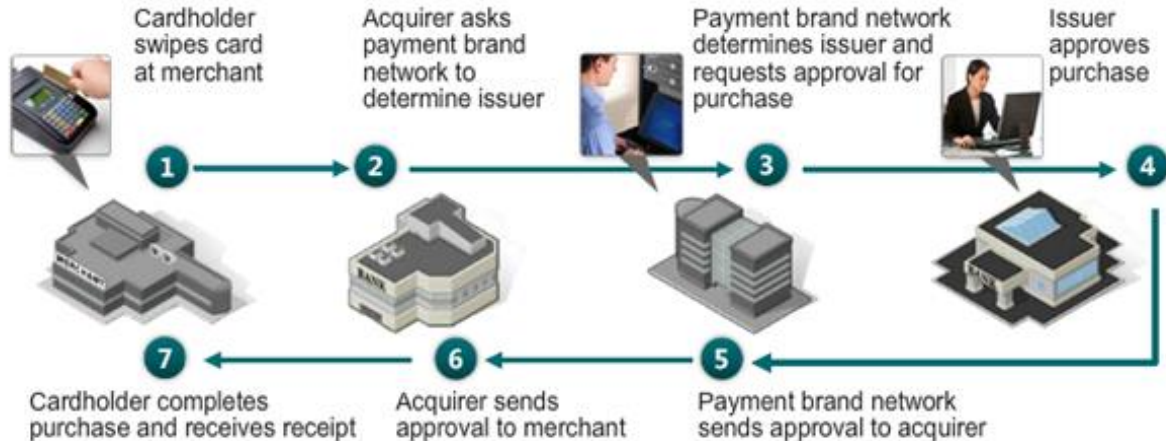
- Organization accepting the payment card for payment during a purchase

Acquirer

- Bank or entity the merchant uses to process their payment card transactions
- Receive authorization request from merchant and forward to Issuer for approval
- Provide authorization, clearing, and settlement services to merchants
- Acquirer is also called:
 - Merchant Bank
 - ISO (sometimes) independent sales organization
 - Payment Brand - Amex, Discover, JCB
 - Never Visa or MasterCard



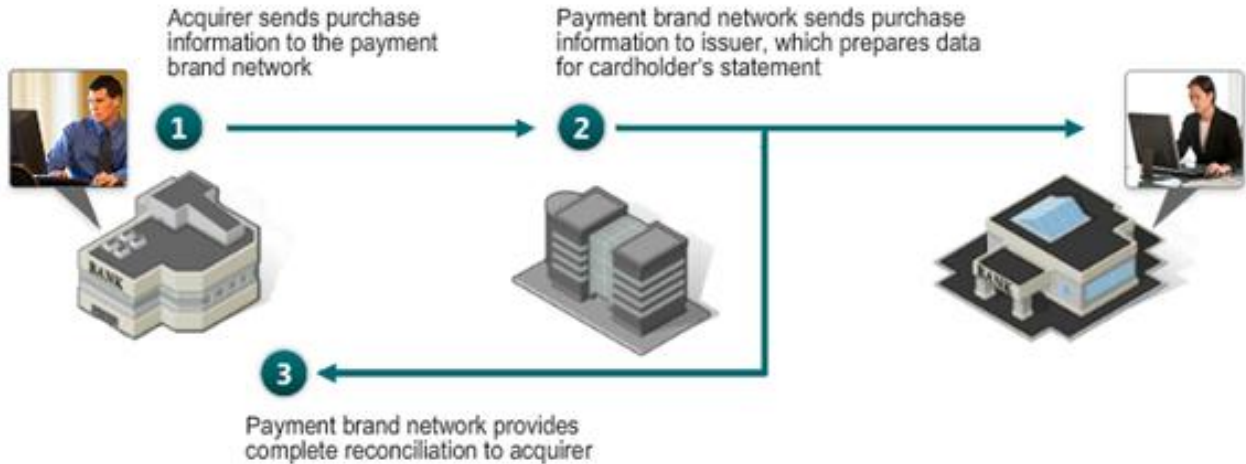
The Basics - Authorization



Authorization (Time of Purchase)

- Merchant requests and receives authorization from the Issuer to allow the purchase to be conducted.
- Authorization Code is provided.

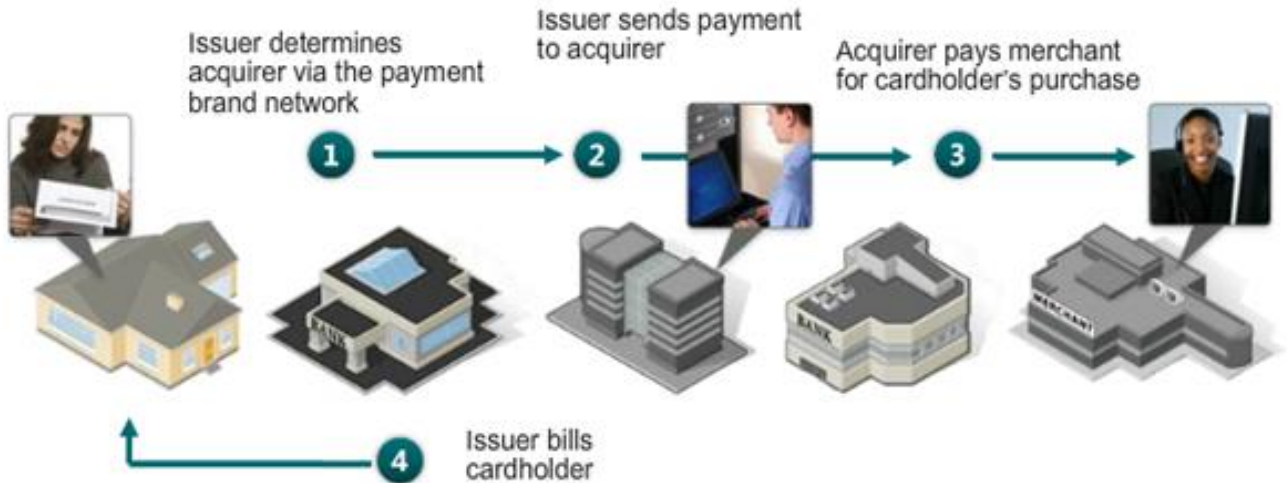
The Basics - Clearing



Clearing (Usually within one day)

- Acquirer and Issuer exchange purchase information

The Basics - Settlement



Settlement (Usually within two days)

- Acquirer pays merchant for cardholder purchase
- Issuer bills cardholder

Merchants and Service Providers

- Merchant
 - Entity that accepts payment cards bearing the logos of any of the five members of PCI SSC as payment for goods and/or services.
- Service Provider
 - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.



PCI Merchant Levels

Merchant Level	Merchant Definition	Compliance
Level 1	More than 6 million V/MC transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 2	1,000,000 – 5,999,999 V/MC transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 3	20,000 – 1,000,000 V/MC e-commerce transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 4	Less than 20,000 e-commerce V/MC transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing



PCI Service Provider Levels

Service Provider Level	Service Provider Definition	Compliance
Level 1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year.	Annual Onsite PCI Data Security Assessment, Quarterly Network Scans, Annual External and Internal Penetration Testing, Quarterly Wireless Testing
Level 2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year.	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing, Quarterly Wireless Testing



Complying with PCI

Compliance VS. Certification (reporting)

Every organization that stores, processes, or transmits credit card data needs to comply with all DSS standards.

Depending on the type and size of the organization you must annually certify compliance utilizing either a self assessment questionnaire (SAQ) or independent third party review and Report on Compliance (ROC).



PCI DSS Self-Assessment Questionnaire (SAQ)

The PCI DSS SAQ consists of two components:

1. Questions corresponding to the PCI DSS requirements
 - Appropriate to service providers and merchants
2. Attestation of Compliance
 - Organization certification of eligibility to perform and have performed the appropriate Self-Assessment. The correct Attestation will be packaged with the SAQ selected.



Types of Self Assessment Questionnaires

There are eight SAQ categories:

A Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.

B Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage

C-VT Merchants using **only web-based virtual terminals**, no electronic cardholder data storage

C Merchants with **payment application systems connected to the Internet**, no electronic cardholder data storage

D All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.



Types of Self Assessment Questionnaires

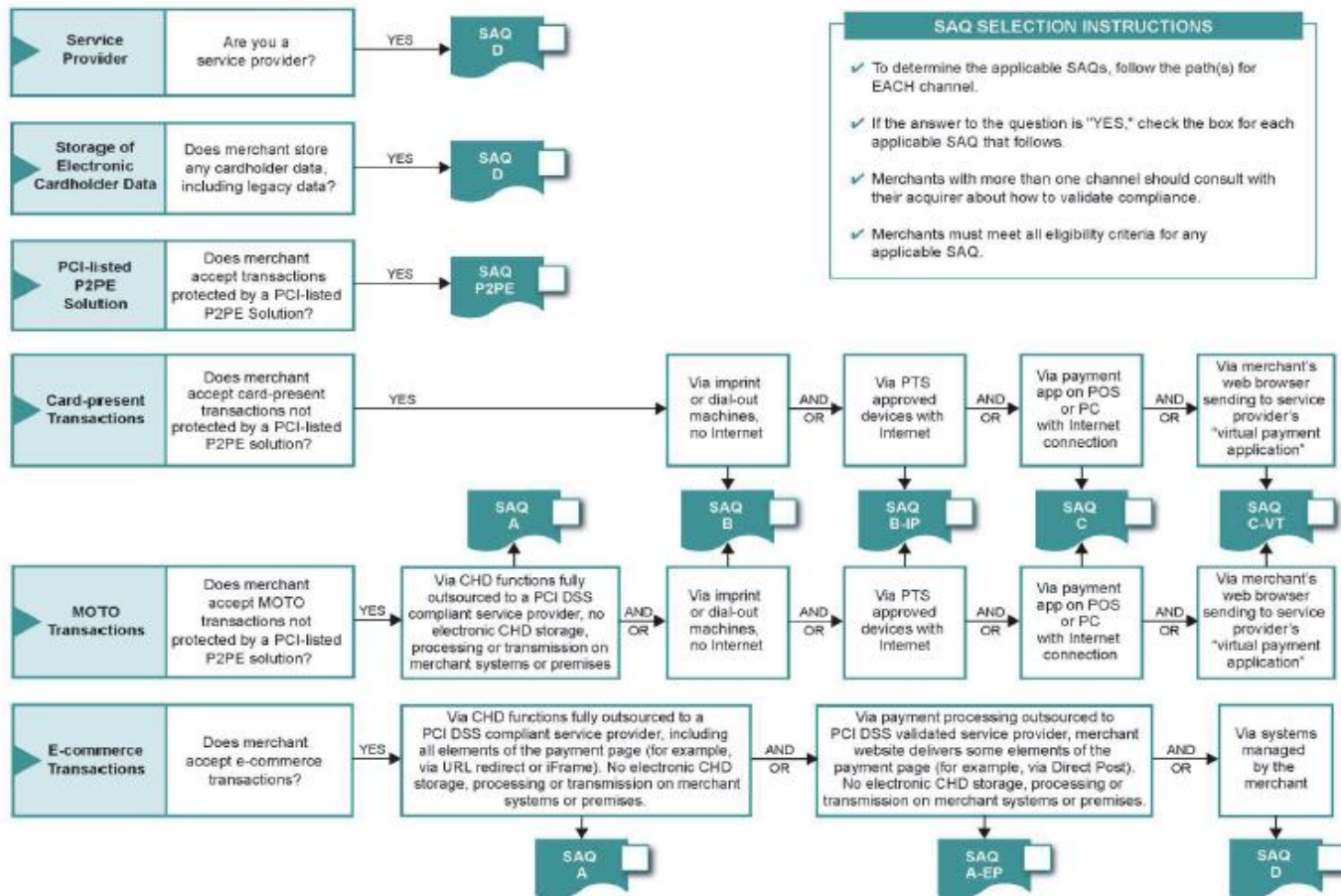
P2PE Merchants who have implemented a validated Point-to-Point Encryption Solution that is listed on the PCI SSC website (Not applicable to e-commerce channels)

A-EP E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchants systems or premises.
(applicable only to e-commerce channels)

B-IP Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.



Which SAQ Best Applies to My Environment?



- https://www.pcisecuritystandards.org/documents/SAQ_InstrGuidelines_v3-1.pdf



How to Scope a PCI DSS Assessment

How does the organization receive card holder data?

How many applications store, process, or transmit cardholder data?

How many databases platforms are used to store cardholder data (e.g. Oracle, MS SQL, DB2)?

How many servers are used to store, process or transmit cardholder data?

What are the operating systems for each of the servers (e.g. MS, UNIX, Linux, AS400, etc...)?

Is there segmentation between the systems with cardholder data and the rest of the network?

How is segmentation achieved (e.g. VLAN, Firewall, etc...)?

How many Internet, DMZ, or segmentation firewalls are in place?



How to Scope a PCI DSS Assessment

Is wireless technology in use anywhere on the network?

If so, in how many locations?

Is cardholder data transmitted over wireless devices at any point?

Are payment card transactions accepted through a web server?

Is PAN or other cardholder data stored on the POS systems for any length of time?

How many data centers store, process or transmit cardholder data?

How many call centers store, process or transmit cardholder data?

Is any part of the environment outsourced?

Are there third parties, outsourcers, or business partners connected to the network?



Overview – PCI DSS – “Digital Dozen”

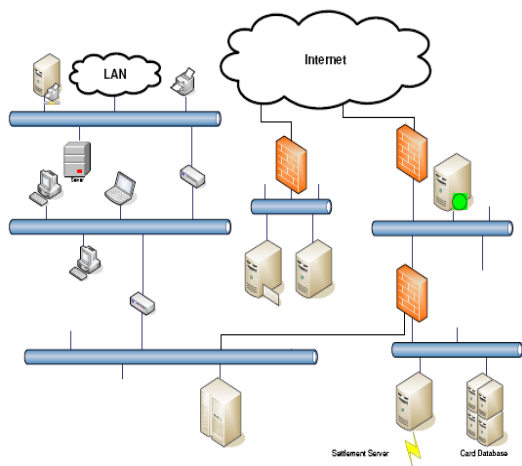
PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. 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 data 4. 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 programs 6. 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 know 8. Identify and authenticate access to system components 9. 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 data 11. 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



PCI DSS – Build & Maintain a Secure Network

	Goals	PCI DSS Requirements
1	Build and Maintain a Secure Network	<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



Default password lists:

- <http://www.phenoelit-us.org/>
- <http://www.cirt.net/passwords>
- www.google.com

➤ “default password”

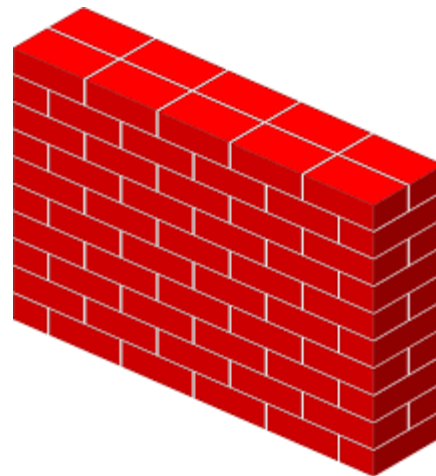
PCI DSS – Build & Maintain a Secure Network

Requirement 1

Build and Maintain a Secure Network and Systems

REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data

- Firewalls control traffic between an entity's internal networks and **untrusted networks**, as well as traffic into and out of **sensitive areas** such as the entity's cardholder data environment.
- Firewalls examine and control all network traffic while blocking transmissions that do not meet the specified rules that exist within the firewall's configuration settings.
- All systems within the cardholder data environment must be protected from unauthorized access from any untrusted networks, and firewalls play a key role in providing such protection.



***Note:** Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1.*

PCI DSS – Build & Maintain a Secure Network

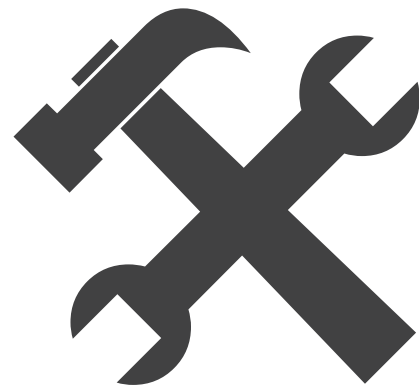
Requirement 2

Build and Maintain a Secure Network and Systems

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

The controls covered in Requirement 2 include:

- Not using vendor-supplied **default passwords**,
- Utilizing system configuration standards for all components,
- Maintaining an inventory of system components, and
- Ensuring all non-console access to network devices, servers, and other components is encrypted.



PCI DSS – Protect Cardholder Data

	Goals	PCI DSS Requirements
2	Protect Cardholder Data	<div>3. Protect stored cardholder data</div> <div>4. Encrypt transmission of cardholder data across open, public networks</div>

- Minimize storage
 - Implement data retention and disposal policies
 - Do NOT store sensitive authentication data
 - Mask displayed PAN
 - Render PAN unreadable where stored
 - Protect cryptographic keys
- **ADDITION: NEVER send unprotected PAN by end user messaging (email, chat, IM, etc...)**



PCI DSS – Protect Cardholder Data

Requirement 3

Protect Cardholder Data

REQUIREMENT 3: Protect Stored Cardholder Data

- Protect stored data; specifically primary account number (PANs) and sensitive authentication data (SAD).
- Minimize risk associated with the storage of cardholder data.

If you don't need it, don't store it!



PCI DSS – Protect Cardholder Data

Requirement 4

Protect Cardholder Data

REQUIREMENT 4: Encrypt transmission of cardholder data across open, public networks

- Protection of cardholder data during transmission over networks that may be easily accessed or breached by malicious individuals.
- Minimize risk associated with transmission of cardholder data over open, public networks.



PCI DSS – Maintain Vulnerability Mgmt Program

	Goals	PCI DSS Requirements
3	Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs
		6. Develop and maintain secure systems and applications

- “Use anti-virus...”
- Secure software development and change control...
- Secure build checklists:
 - CIS offers vendor-neutral hardening resources
<http://www.cisecurity.org/>
 - Microsoft Security Checklists
<http://www.microsoft.com/technet/archive/security/chklist/default.mspx?mfr=true>
<http://technet.microsoft.com/en-us/library/dd366061.aspx>
 - PA-DSS “certified” applications will have an Implementation Guide



PCI DSS – Maintain Vulnerability Mgmt Program

Requirement 5

Maintain a Vulnerability Management Program

*REQUIREMENT 5: Protect all systems against malware and regularly update **anti-virus** software or programs*

- Protection from **malicious software**
- Ensure proper use of anti-virus technologies to minimize the risks associated with malicious code



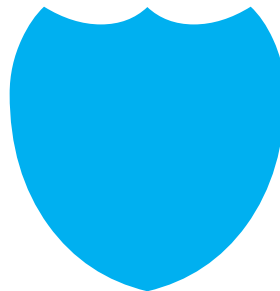
PCI DSS – Maintain Vulnerability Management Program

Requirement 6

Maintain a Vulnerability Management Program

REQUIREMENT 6: Develop and maintain secure systems and applications

- Protection from exploitation of vulnerabilities
- Develop secure applications and systems
- Ensure security patches and secure system and application configurations are managed properly



PCI DSS – Implement Strong Access Controls

	Goals	PCI DSS Requirements
4	Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
		8. Assign a unique ID to each person with computer access
		9. Restrict physical access to cardholder data

- Principle of minimum access and least privilege
- Unique IDs (→ NO shared IDs)
- Long/strong passwords, password controls, strong authentication
- **Password protected screen saver time outs (15 min)**
- Limit and monitor physical access
- Secure storage and tracking of media

PCI DSS – Implement Strong Access Controls

Requirement 7

Implement Strong Access Control Measures

REQUIREMENT 7: Restrict access to cardholder data by business need to know

- Control all access to cardholder data.
- Ensure only individuals with a business or job “need to know” are granted access.



PCI DSS – Implement Strong Access Controls

Requirement 8

Implement Strong Access Control Measures

REQUIREMENT 8: Identify and authenticate access to system components.

- Assign a unique ID and authentication to each person with access.
- Ensures that individuals are uniquely accountable for their actions.



PCI DSS – Implement Strong Access Controls

Requirement 9

Implement Strong Access Control Measures

REQUIREMENT 9: Restrict physical access to cardholder data

- Control physical access to all systems in the CDE that store, process, or transmit cardholder data.
- For Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity’s premises.
- A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.
- “Media” refers to all paper and electronic media containing cardholder data.



PCI DSS – Regularly Monitor and Test Networks

	Goals	PCI DSS Requirements
5	Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
		11. Regularly test security systems and processes

- Process, system, and application logging
- Secure the audit logs
- Review and retain audit logs
- Regular testing:
 - Quarterly*: Wireless testing & Vulnerability scanning
 - Annual*: Penetration testing
- IDS/IPS and
- File integrity monitoring



PCI DSS – Regularly Monitor and Test Networks

Requirement 10

Regularly Monitor and Test Networks

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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong.



PCI DSS – Regularly Monitor and Test Networks

Requirement 11

Regularly Monitor and Test Networks

REQUIREMENT 11: Regularly test security systems and processes.

Test system components, applications, processes, and security controls to ensure the current environment is secure from all known vulnerabilities, threats, attack-vectors, etc.



PCI DSS – Maintain Information Security Policy

	Goals	PCI DSS Requirements
6	Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Section	Control Domain
Section 1	Organization Administration
Section 2	Vendor Administration
Section 3	Technical Infrastructure Administration
Section 4	Data Administration
Section 5	Software Administration
Section 6	Application Administration
Section 7	User Account Administration
Section 8	IT Operations & Support Administration
Section 9	Physical Environment Administration
Section 10	Incident Response – Business Continuity – Disaster Recovery



DSS 3.2 to DSS 3.2.1

Highlighted Changes

- Addressed minor punctuation and format issues.
- SSL/early TLS migration effort, as the migration date of July 1, 2018 has passed.
- PCI DSS continues to be updated to be relevant to known risks.
 - PCI Software Security Framework (PCI SSF)





How PCI Relates to Credit Unions

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

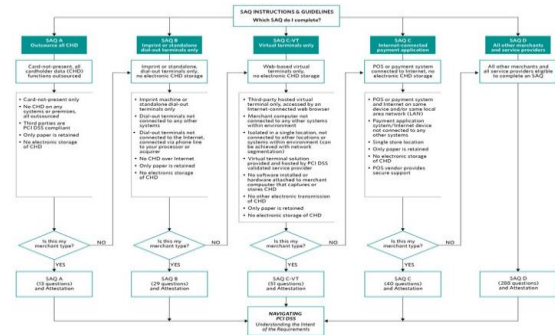
Exercise

- Think about how your credit union stores, processes, or transmits credit card information
- Think in terms of the steps/stages followed
 - Examples:
 - ◇ Accept payment information over the phone
 - ◇ Members make payments online
 - ◇ Receive payment information in the mail
 - ◇ Member statements are sent/stored/reviewed by member services reps
- End Goal is to understand “where the card data lives”



Understand Where Your Data Lives

- Develop data inventory
 - Payment/data flow
 - Where static data resides
- Who is mining data and for what purposes
- Understand how the back up system works



Exercise

- Do you accept CC payment “in-person”?
- Do you accept CC payment over the phone?
- Do you accept CC payment via a website?
- Do you rely on a 3rd party/vendor to host or manage any of your data systems?
- Do you store or process CC data for someone else?
- Do you have instant issue capabilities?
- Are ATMs “on your network”?



Most Significant Challenges to PCI Compliance?

7. Identify where card holder data is “stored”
6. Compare current control requirements to PCI – identify overlaps and gaps
5. Secure application development/compliance
4. Vulnerability management and remediation
3. Secure standard configuration management
2. Network segmentation
1. Operational maturity:
 - Disciplined adherence to policies and procedures
 - Mature documented exception management process



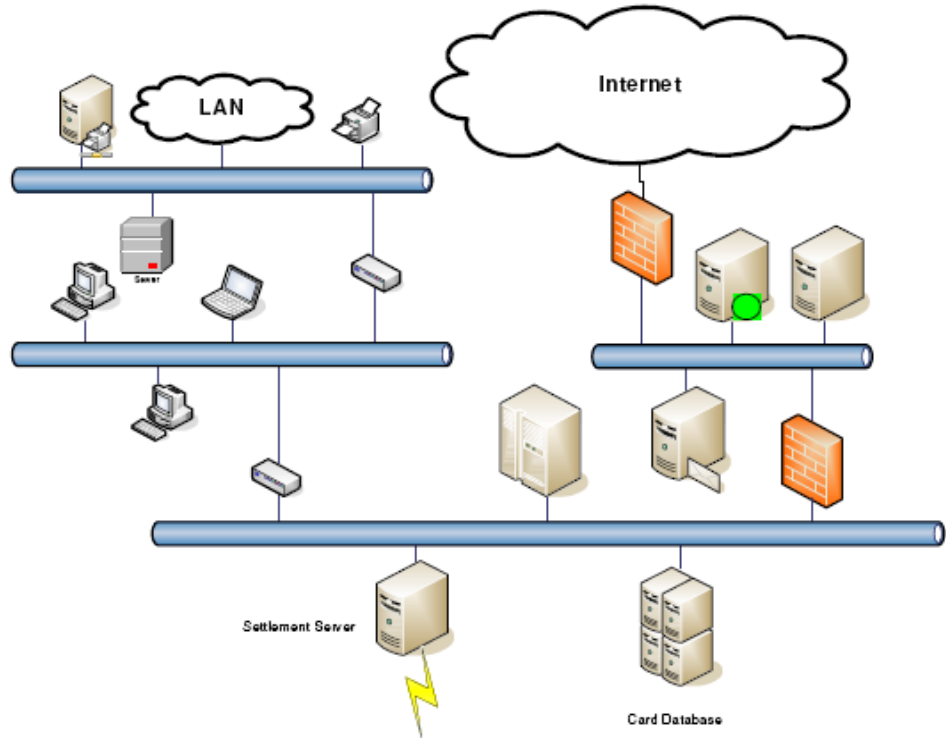
Common Struggles for Credit Unions

- Isolation/segmentation is difficult
 - Everything talks with the core
 - This makes all systems on the network in scope



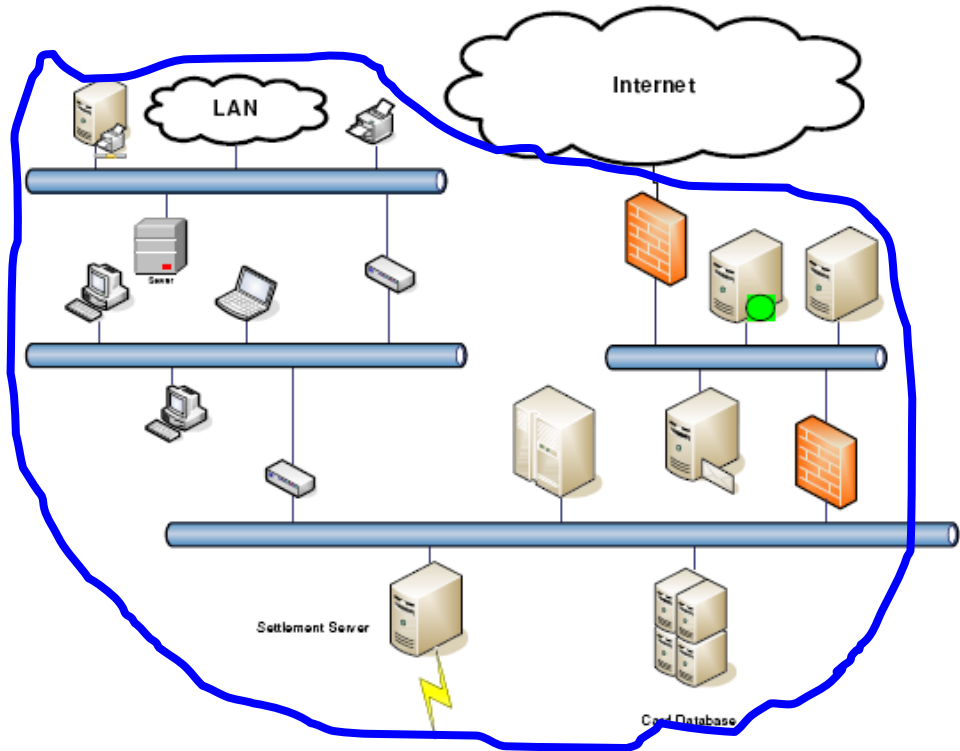
Exercise - Segment Your Network

- What is in-scope here?
- NOTHING
- Firewalls
- Servers
- PCs
- Everything
- Why?



Exercise - Segment Your Network

- What is in-scope here?
- NOTHING
- Firewalls
- Servers
- PCs
- Everything
- Why?

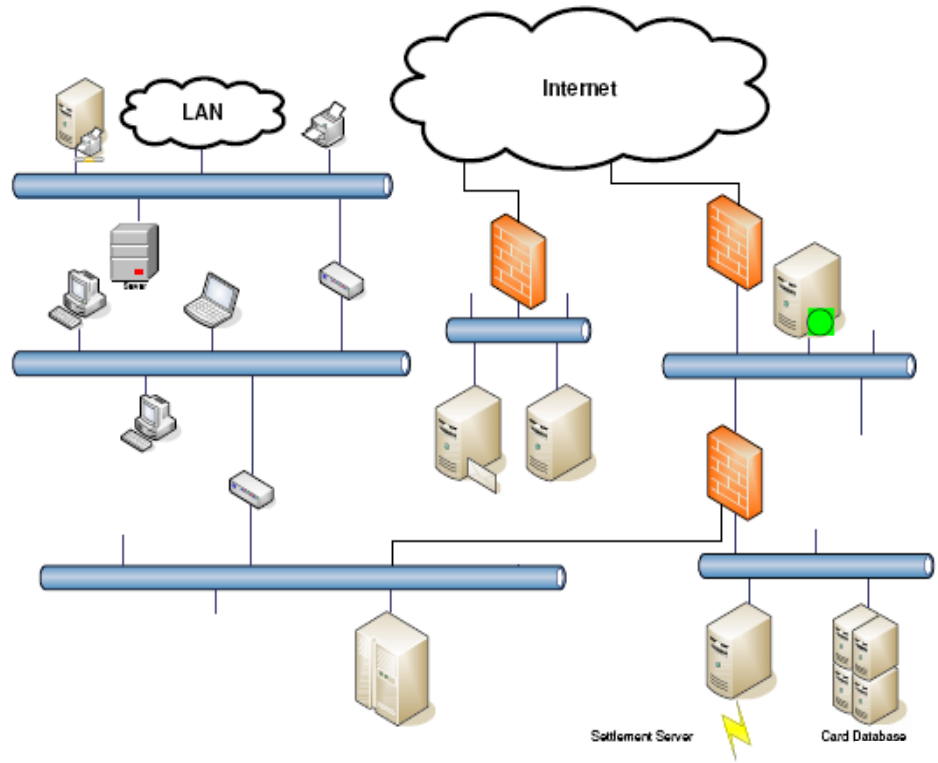


Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?

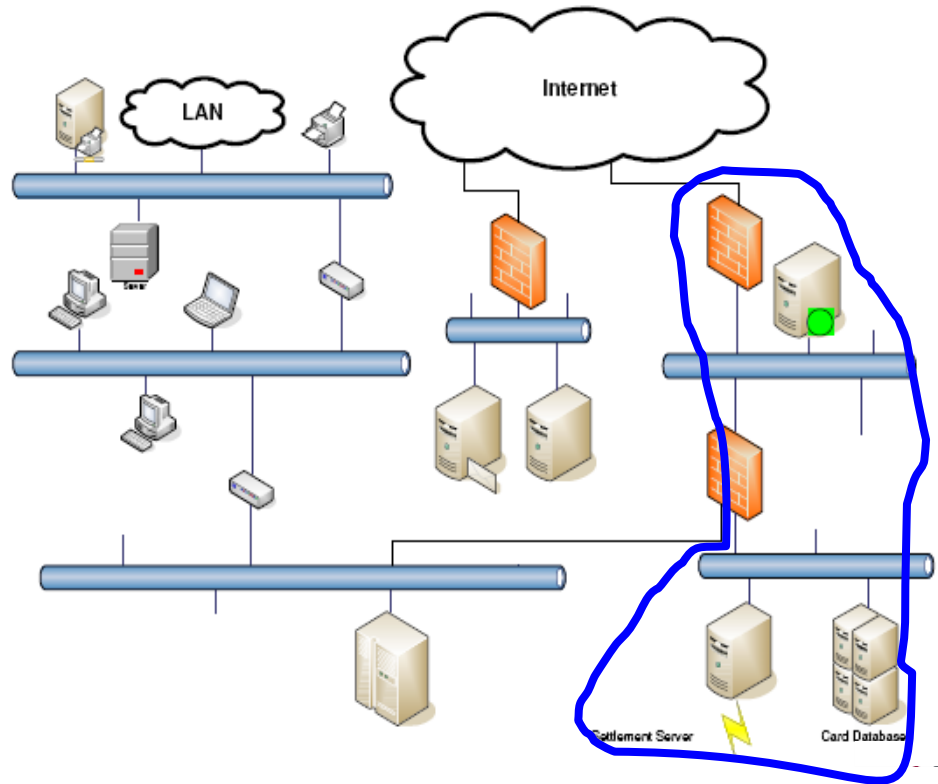


Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?



Common Struggles for Credit Unions

- Reports (PDF, XLSX, etc.) contain PAN
 - Core/vendor software generates reports with PAN data
 - These reports exist in email and on network file shares
- Data warehouse and analytics...



Common Struggles for Credit Unions

- Card data is received over the phone
 - Service center records phone calls
 - Phone calls contain PAN data



Common Struggles for Credit Unions

- Vendor software doesn't follow PCI guidelines
 - Instant issue systems store SAD
 - Vendor software stores clear-text PAN
 - Etc.



Common Struggles for Credit Unions

- Members have old systems
 - Credit Union wants to support legacy (non-compliant) protocols for members with old PCs



Summarize

1. Credit unions need to be PCI compliant
2. There is no “PCI Police” looking for you
3. Some examiners are starting to ask about compliance status
4. Most Credit Unions are both Merchants and Service Providers
 - Could be Level 1 or Level 2 service provider



Summarize

5. You need to complete SAQ-D
 - All 400+ controls are in scope and need to be reviewed
6. You most likely are not compliant right now
7. Start the process to self-assess your own compliance status



Summarize

8. Where to start?

- Identify where card data lives and how it flows through environment
- Update policies and processes to address PCI requirements
- Follow PCI Prioritized Approach



Questions





“Information technology and business are becoming inextricably interwoven. I don’t think anybody can talk meaningfully about one without talking about the other.”
-Bill Gates

Randy Romes, CISSP, CRISC, CISA, MCP, PCI-QSA
Managing Principal – Cybersecurity Services Team

randy.romes@CLAconnect.com
612.397.3114 – office
612.554.3967 - cell



June 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Cloud Cyber Security



Create Opportunities
We promise to know you and help you.

CLA – A Professional Services Firm

- A professional services firm with three distinct business lines
 - Wealth Advisory
 - Outsourcing
 - Audit, Tax, and Consulting
- More than 6,500 employees
- Offices coast to coast
- Serve more than 1,500 financial institutions



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.



Cyber Security Capabilities

Information Security offered as specialized service offering for over 20 years

- Largest Credit Union Service Practice*
- Penetration Testing and Vulnerability Assessment
 - Red Team, Black Box, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance (GLBA, FFIEC, CIS, etc...)
- PCI-DSS Readiness and Compliance Assessments
- Incident response and forensics
- Cybersecurity architecture
- Independent security consulting
- Internal audit support



*Callahan and Associates 2018 Guide to Credit Union CPA Auditors.



C:\whoami

- “Professional Student”
- Science Teacher/Self Taught Computer Guy
- IT Consultant - Project Manager → IT Staff/Help Desk → Hacker
- Assistant Scout Master (Boy Scouts)



Raise Your Hand If...



amazon tap
ALEXA-ENABLED
PORTABLE SPEAKER

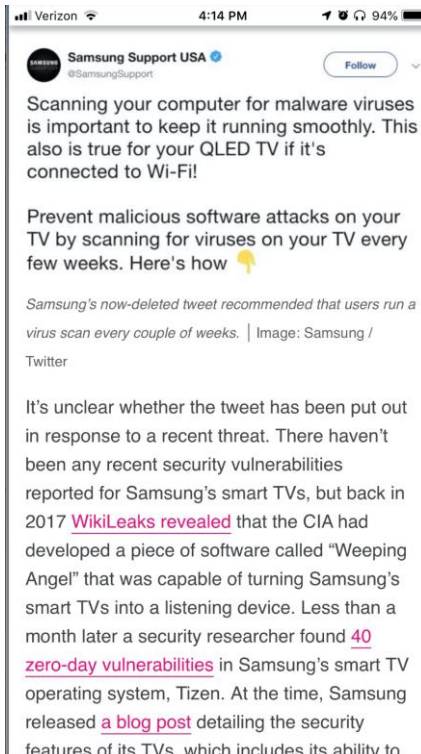
JUST TAP & ASK



Cloud Computing, Compute Model for a Smarter Planet
Globalization and Globally Available Resources



When a TV is NOT a TV...

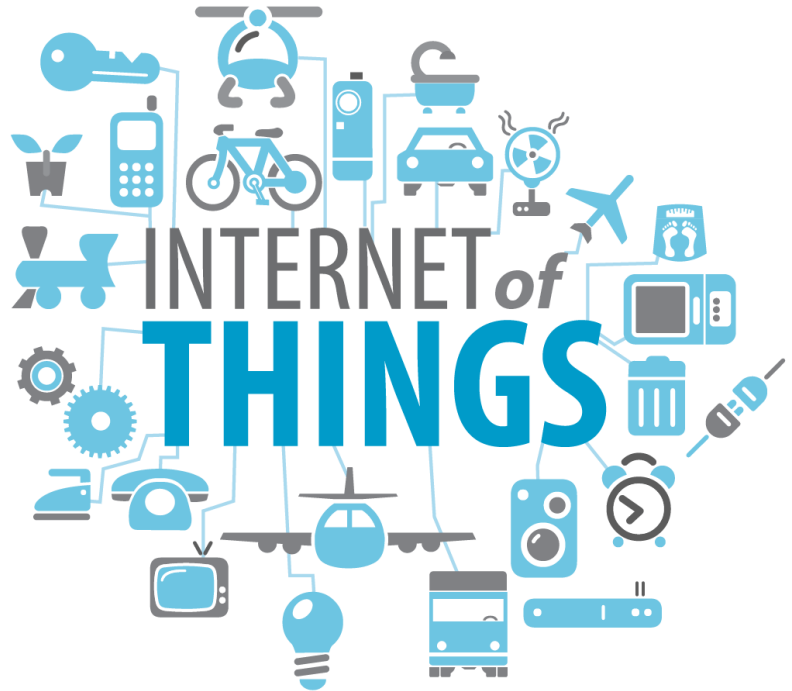


<https://www.theverge.com/2019/6/17/18681683/samsung-smart-tv-virus-scan-malware-attack-tweet>



Everything Can Talk to Everything....

- Security cameras
 - HVAC systems
 - Door sensors and proximity readers
 - “Chrome wants to remember your location...”
 - “Hey Alexa, what’s my balance?”
- **“Presence”**





Sun Tzu:

*“Know your enemy and
know yourself and you can
fight a hundred battles
without disaster”*

The Current State of Cybercrime

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an
SEC-registered investment advisor

What is the Cloud – The Old Cloud

- The original “cloud computing”:



What is the Cloud – The New Cloud

- Today's cloud: Hosted service or process all the way to hosted infrastructure.

Amazon Web
Services

Microsoft
Azure

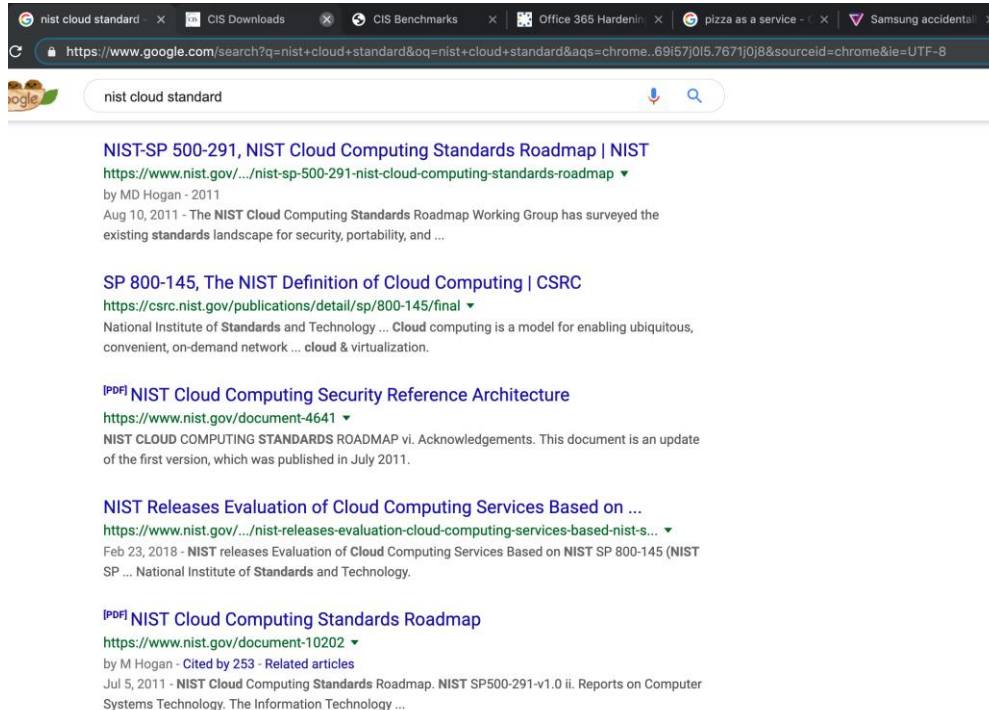
Google Apps

Drop Box

vmware



Google... NIST Cloud Standard



The screenshot shows a Google search for "nist cloud standard". The search bar contains the text "nist cloud standard". Below the search bar, several search results are displayed:

- NIST-SP 500-291, NIST Cloud Computing Standards Roadmap | NIST**
<https://www.nist.gov/.../nist-sp-500-291-nist-cloud-computing-standards-roadmap> ▼
 by MD Hogan - 2011
 Aug 10, 2011 - The NIST Cloud Computing Standards Roadmap Working Group has surveyed the existing standards landscape for security, portability, and ...
- SP 800-145, The NIST Definition of Cloud Computing | CSRC**
<https://csrc.nist.gov/publications/detail/sp/800-145/final> ▼
 National Institute of Standards and Technology ... Cloud computing is a model for enabling ubiquitous, convenient, on-demand network ... cloud & virtualization.
- [PDF](#) NIST Cloud Computing Security Reference Architecture**
<https://www.nist.gov/document-4641> ▼
 NIST CLOUD COMPUTING STANDARDS ROADMAP vi. Acknowledgements. This document is an update of the first version, which was published in July 2011.
- NIST Releases Evaluation of Cloud Computing Services Based on ...**
<https://www.nist.gov/.../nist-releases-evaluation-cloud-computing-services-based-nist-s...> ▼
 Feb 23, 2018 - NIST releases Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP ... National Institute of Standards and Technology.
- [PDF](#) NIST Cloud Computing Standards Roadmap**
<https://www.nist.gov/document-10202> ▼
 by M Hogan - Cited by 253 - Related articles
 Jul 5, 2011 - NIST Cloud Computing Standards Roadmap. NIST SP500-291-v1.0 ii. Reports on Computer Systems Technology. The Information Technology ...



Standards Have Been In Place...

National Institute of Standards and Technology (NIST) definition of cloud computing published October 7, 2009:

“Cloud computing is a model for enabling convenient, on-demand network access to **a shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

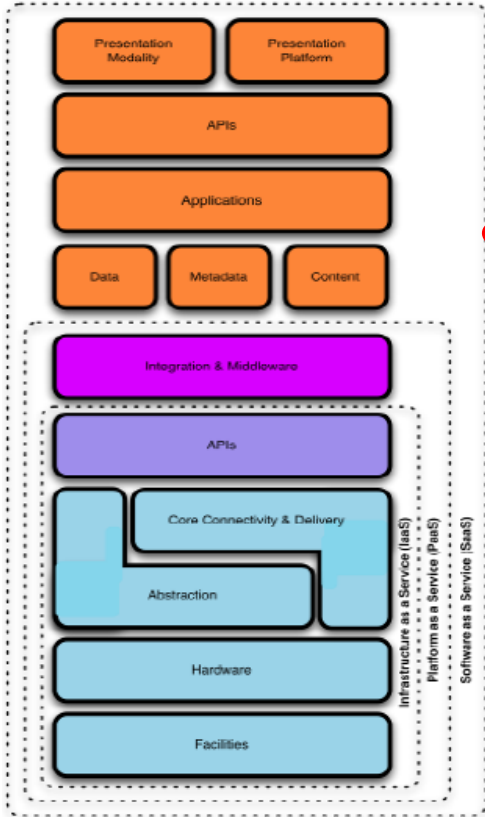


Three Cloud Computing Service Models

- Software as a Service (SaaS)
 - Capability to use the provider's applications that run on the cloud infrastructure.
- Platform as a Service (PaaS)
 - Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider
- Infrastructure as a Service (IaaS)
 - Capability to provision processing, storage, networks and other fundamental computing resources that offer the customer the ability to deploy and run arbitrary software, which can include operating systems and applications



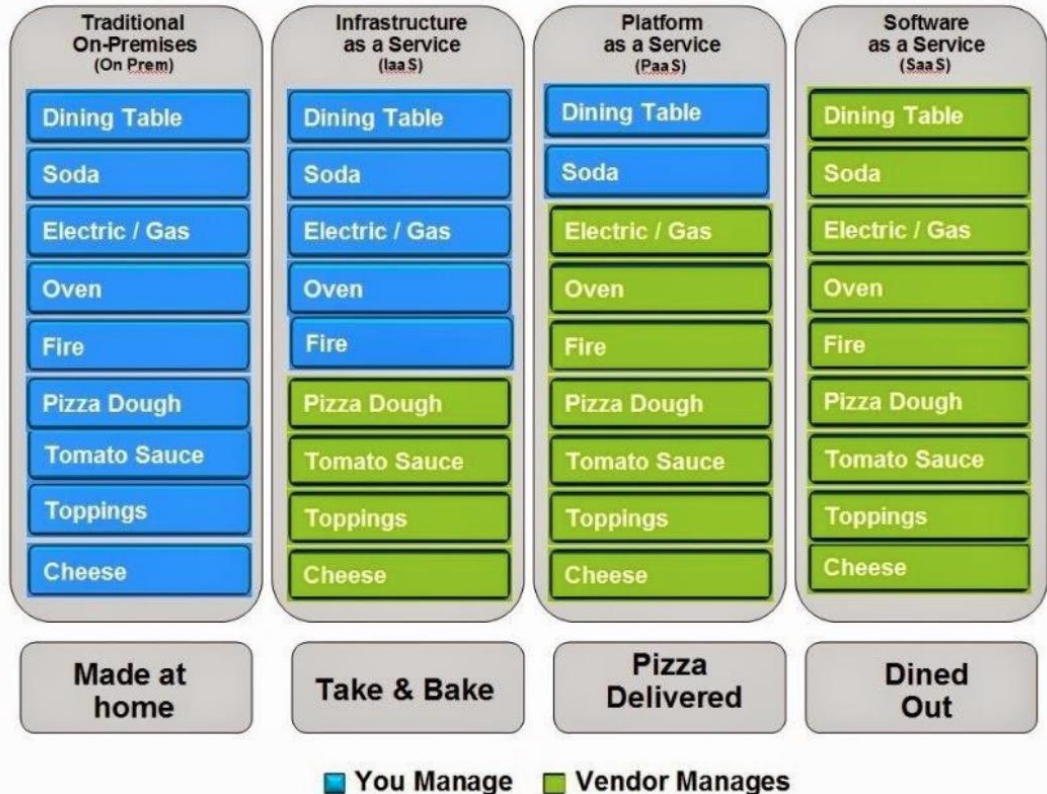
Cloud Computing Service Models



- Multi-tenancy...
- The lower down the stack the cloud service provider stops --
- The more capabilities and management the users are responsible for implementing and managing themselves

Cloud Pizza?

Pizza as a Service



Cloud Computing Controls

- Cloud computing means:
 - An increased need for good policies
 - Clear communication between the provider and the consumer of the services
 - **Understanding of providers responsibilities and your responsibilities**
 - Ownership and governance of the relationship with the provider.



Cloud Computing Deployment Models

- **Private cloud:** *(You probably already have this...)*
 - Operated solely for an organization
- **Community cloud:**
 - Shared by several organizations
 - Supports a specific community that has a shared mission or interest
- **Public cloud:** *(You are probably using this...)*
 - Made available to the general public or a large industry group
 - Owned by an organization that sells cloud services
- **Hybrid cloud:**
 - Composed of two or more clouds (private, community or public) that remain unique entities



Cloud Computing Controls

- The overall control domains are the same as an in house IT environment

➤ **The challenge is to figure out who is doing what**

➤ **YOU are still responsible...**

Domain	Focus
Organization and Management Controls	<ul style="list-style-type: none"> • IT Organization & Governance • Policies, Standards & Guidelines • Personnel Administration • Vendor Administration, including External Dependency Management • Technology Administration • Cyber Risk Management & Oversight • Threat Intelligence & Collaboration
Technical Infrastructure	<ul style="list-style-type: none"> • Technical Documentation & Illustration(s) • Network Administration • Server Administration • Workstation Administration • Peripheral Administration • Cybersecurity Controls
Software Administration	<ul style="list-style-type: none"> • Software Asset Administration • Software Development Administration • Software Change Management
Data Administration	<ul style="list-style-type: none"> • Data Management • Database Administration (<i>If Applicable</i>) • Data Transfer(s) Administration • Data Storage & Backup Administration
Application Administration (For Each "In Scope" Application)	<ul style="list-style-type: none"> • Access Controls & Permissions • Business Rules/Parameters • Data Input/Processing/Output • Data Maintenance • Activity Logging/Monitoring
IT Operations & Support	<ul style="list-style-type: none"> • User Account Administration • IT Systems Operations • Problem Management (<i>Help Desk</i>)
Physical Environment	<ul style="list-style-type: none"> • Physical Security • Environment Controls
Business Continuity	<ul style="list-style-type: none"> • Incident Response Management and Resilience • Disaster Recovery



Cloud Computing Controls

- Controls in the cloud computing environment may be provided by the consumer/company, the cloud service provider, or a separate 3rd party.
- SSAE 16/18 SOC2 report from service providers



Cloud Computing

Activity :

- Describe an outsourced (cloud) IT service relationship in place at your credit union
 - What do they do/manage for you (data, processes, etc...)
 - How do they interact with you
 - What are the service provider's responsibilities and what your credit union staff's responsibilities
 - What is the Service Model
 - What is the Deployment Model



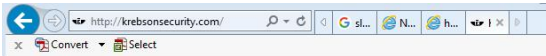
Cloud Computing

Activity :

- Describe an outsourced (cloud) IT service relationship in place at your credit union
 - What security measures do you think/assume they now take care of for you?
 - Who at the credit union is an expert for your credit unions cloud based system?
(Are they an engineer, mechanic, or uber driver?)



Internet of Things (IoT)



Other — 45 comments

13 IoT Devices as Proxies for Cybercrime

OCT 16

Multiple stories published here over the past few weeks have examined the **disruptive power** of hacked “Internet of Things” (IoT) devices such as **routers, IP cameras and digital video recorders**. This post looks at how crooks are using hacked IoT devices as proxies to hide their true location online as they engage in a variety of other types of cybercriminal activity — from frequenting underground forums to credit card and tax refund fraud.



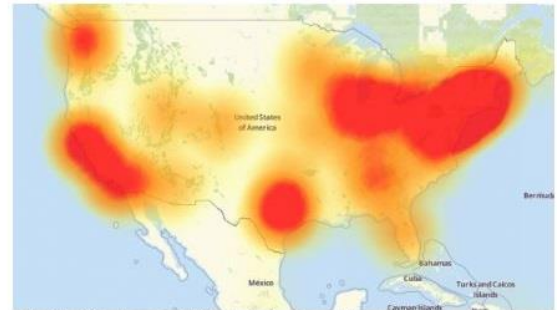
Recently, I heard from a cybersecurity researcher who'd created a virtual “honeypot” environment designed to simulate hackable IoT devices. The source, who asked to remain anonymous, said his honeypot soon began seeing traffic destined for **Asus** and **Linksys** routers running default credentials. When he examined what that traffic was designed to do, he found his honeypot systems were being told to download a piece of malware from a destination on the Web.

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including **Twitter**, **Amazon**, **Tumblr**, **Reddit**, **Spotify** and **Netflix**.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downtime.com.

At first, it was unclear who or what was behind the attack on Dyn. But over the past few hours, at least one computer security firm has come out saying the attack involved **Mirai**, the same malware strain that was used in the **record 620 Gbps attack on my site last month**. At the end September 2016, the hacker responsible for creating the Mirai malware released the source code for it, effectively letting anyone build their own attack army using Mirai.

Mirai scours the Web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users.

According to researchers at security firm **Flashpoint**, today's attack was launched at least in part by a Mirai-based botnet. **Allison Nixon**, director of research at Flashpoint, said the botnet used in today's ongoing attack is built on the backs of hacked IoT devices — mainly compromised digital video recorders (DVRs) and IP cameras made by a Chinese hi-tech company called **XiongMai Technologies**. The components that XiongMai makes are sold



Internet of Things (IoT)

- These “Things” are “computers”
- They have software that needs to be updated
- They provide remote access and control
- They have presence and sensing
- They are sending and receiving data
- Examples include:
 - _____
 - _____

26 P2P Weakness Exposes Millions of IoT Devices

APR 19

A peer-to-peer (P2P) communications technology built into millions of security cameras and other consumer electronics includes several critical security flaws that expose the devices to eavesdropping, credential theft and remote compromise, new research has found.



A map showing the distribution of some 2 million iLinkP2P-enabled devices that are vulnerable to eavesdropping, password theft and possibly remote compromise, according to new research.

The security flaws involve **iLinkP2P**, software developed by China-based **Shenzhen Ynni Technology**. iLinkP2P is bundled with millions of Internet of Things (IoT) devices, including security cameras and Webcams, baby monitors, smart doorbells, and digital video recorders.

iLinkP2P is designed to allow users of these devices to quickly and easily access them remotely from anywhere in the world, without having to tinker with one's firewall: Users simply download a mobile app, scan a barcode or enter the six-digit ID stamped onto the bottom of the device, and the P2P software handles the rest.



<https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/>

Examples closer to home...

- Business Email Compromise
- Persuasion Attack
- RDP compromise... leads to Ransomware





The Boy Scouts Motto:

“Be Prepared”

Strategies and Action Items

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

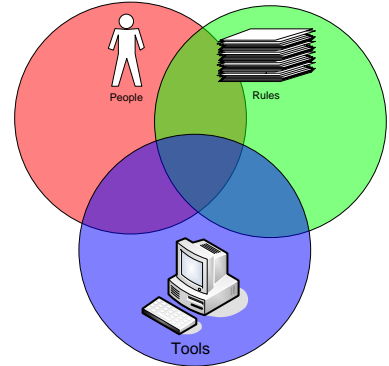
Strategies

Our information security strategy should have the following objectives:

- Users who are aware and savvy
- Systems that are hardened and resistant to malware and attacks
- Resilience Capabilities: Monitoring, Incident Response, Testing, and Validation



Policies and Standards



- People, Rules and Tools
 - What do we expect to occur?
 - How do we conduct business?

- Standards based operations from a governance or compliance framework:
 - GLBA/FFIEC, NCUA 748 A&B, etc...
 - PCI – DSS
 - CIS Critical Controls, NIST, ISO

Standards Based Operations



CIS Controls™

V7

©2018 CliftonLarsonAllen LLP

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>



Create Opportunities | We promise to know you and help you.

CIS Benchmarks



With our global community of cybersecurity experts, we've developed CIS Benchmarks: 100+ configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats.



©2018 CliftonLarsonAllen LLP

Overview of CIS Benchmarks and CIS-CAT Demo

Register for the CIS Benchmarks Webinar
Nov 27, 2018 at 1:30 PM EST or
Dec 11, 2018 at 9:30 AM EST
[See Webinar Details](#)

[CIS Benchmarks FAQ](#)

[Access all CIS Benchmarks](#)



Operating Systems

Server Software

Cloud Providers

Mobile Devices

Network Devices

Desktop Software

Multi Function Print Devices

Currently showing ALL Technologies. Use the buttons above to filter the list.

Operating Systems

Amazon Linux

[Expand to see related content](#)



[Download CIS Benchmark](#)



CIS Hardened Image and Remediation Kit also available

Linux

Cloud Providers

Amazon Web Services

[Expand to see related content](#)

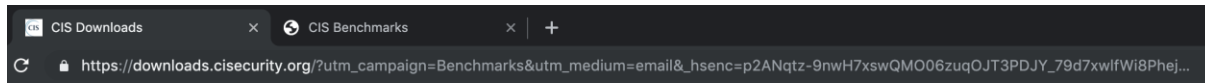


[Download CIS Benchmark](#)



Create Opportunities | We promise to know you and help you.

CIS Cloud Standards and Benchmarks



Cloud Providers

Amazon Web Services

CIS Amazon Web Services Foundations Benchmark v1.2.0

Download PDF

CIS Amazon Web Services Three-tier Web Architecture Benchmark v1.0.0

Download PDF

CIS Amazon Web Services Foundations Benchmark v1.1.0

Download PDF

CIS Amazon Web Services Foundations Benchmark v1.0.0

Download PDF

Google Cloud Computing Platform

CIS Google Cloud Platform Foundation Benchmark v1.0.0

Download PDF

Microsoft Azure

CIS Microsoft Azure Foundations Benchmark v1.1.0

Download PDF

CIS Microsoft Azure Foundations Benchmark v1.0.0

Download PDF



Microsoft Office 365

https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide

Office 365

Filter by title

- Admin home
- Overview
- Setup
- Users and roles
- Email
- Secure your business data
 - Top 10 way to secure your data**
 - Plan for modern authentication
 - Set up multi-factor authentication
 - Set up multi-factor authentication (with Office 2013)
 - GDPR compliance
 - Activity reports and analytics
 - Manage
 - Subscriptions and billing
 - Domains
 - Groups
 - Troubleshoot
 - Get new features
 - Contact support for business products

Download PDF

Top 10 ways to secure Office 365 and Microsoft 365 Business plans

05/14/2019 • 13 minutes to read • Contributors: 🗣️ 📝 🛠️ 📧 all

Tip

Need help with the steps in this topic? We've got you covered. Make an appointment at your local Microsoft Store with an Answer Desk expert to help resolve your issue. Go to the [Microsoft Stores page](#) and choose your location to schedule an appointment.

If you are a small or medium-size organization using one of Microsoft's business plans and your type of organization is targeted by cyber criminals and hackers, use the guidance in this article to increase the security of your organization. This guidance helps your organization achieve the goals described in the Harvard Kennedy School [Cybersecurity Campaign Handbook](#).

Microsoft recommends that you complete the tasks listed in the following table that apply to your service plan.

Task	Office 365 Business Premium	Microsoft 365 Business
1. Set up multi-factor authentication	✓	✓
2. Train your users	✓	✓
3. Use dedicated admin accounts	✓	✓
4. Raise the level of protection against malware in mail	✓	✓
5. Protect against ransomware	✓	✓
6. Stop auto-forwarding for email	✓	✓
7. Use Office Message Encryption		✓
8. Protect your email from phishing attacks		✓
9. Protect against malicious attachments and files with ATP Safe Attachments		✓
10. Protect against phishing attacks with ATP Safe Links		✓

In this article

- 1: Set up multi-factor authentication
- 2: Train your users
- 3: Use dedicated admin accounts
- 4: Raise the level of protection against malware in mail
- 5: Protect against ransomware
- 6: Stop auto-forwarding for email
- 7: Use Office Message Encryption
- 8: Protect your email from phishing attacks
- 9: Protect against malicious attachments and files with ATP Safe Attachments
- 10: Protect against phishing attacks with ATP Safe Links

Is this page helpful?

Yes No



Limit or Disable Remote Access

- The majority of email compromises occur through Outlook web access (OWA). Disabling OWA for the organization or enabling it only on an as-needed, per-user basis offers additional protection to your organization.
- By default, Office 365 allows access via POP3, IMAP, MAPI, EWS, OWA, and ActiveSync for every system user.
 - Users rarely need access using all of these methods.
 - Does your organization use POP3 or IMAP for email connections regularly?
 - If not – disable them.



Require Multi-factor Authentication (MFA)

- The most important thing you can do to protect your organization is to require MFA for users to log in to O365. Microsoft provides guidance for O365 administrators:
 - [Set up multi-factor authentication for Office 365 users](#)
 - [Plan for multi-factor authentication for Office 365 deployments](#)
- Users should select the MFA mobile app for authentication.
 - SMS (text message)-based MFA is **no longer regarded as secure** because of SIM swaps and [other social engineering risks](#).



Manage Message Forwarding

- Cybercriminals often set up inbox rules to forward messages to an external account or to delete messages in order to hide them from the inbox owner. Sometimes the only sign of an account takeover is the presence of unauthorized mailbox rules.
- From an administrative level, you can configure O365 to alert you every time a user sets up a new inbox rule, which can then be followed up on to check the legitimacy of the rule.
- If there isn't a business need for them, it's even more secure to disable forwarding and deletion rules for all users and enable them as needed only for specific users
- [Office 365: Determine accounts that have forwarding enabled](#)



Turn On Audit Logging & Mailbox Auditing

- Without the proper logs, you have to assume the bad actor accessed everything, which can lead to having to provide notification to individuals whose information may not even have been affected.
- To provide useful logs, you need to:
 1. Turn ON audit logging and
 2. Enable mailbox auditing for each user mailbox.
 - By default, audit logging and mailbox auditing are not turned on. Microsoft has plans to change that soon. You need to turn on both *before you experience an incident* for the logs to be helpful.
- [Search the audit log in the Office 365 Security & Compliance Center](#)
- [Enable mailbox auditing in Office 365](#)
- Consider extending the retention time for logs beyond the default 90 days if resources permit.



Tools To Manage Configuration Changes

- Microsoft provides information about how to use Powershell to manage your O365 configuration.
- [Manage Office 365 with Office 365 PowerShell](#)
- [Connect to Office 365 PowerShell](#)
- Other resources to (open-source script) to help automate the process.
- [Secure Your Office 365 Accounts](#)
- <https://github.com/LMGsec/O365-Lockdown>



Disciplined Exception Control, Vulnerability Management and Monitoring

- Monitoring (“built in”)
 - Key system configurations
 - System and application logs
 - Accounts
 - Critical data systems/files
 - Data activity and flow
- Scanning/testing (independent)
 - Patch Tuesday and vulnerability scanning
 - Rogue devices



Passwords

- Good Passwords
- Password Managers
- Two Factor / Multi-Factor Authentication

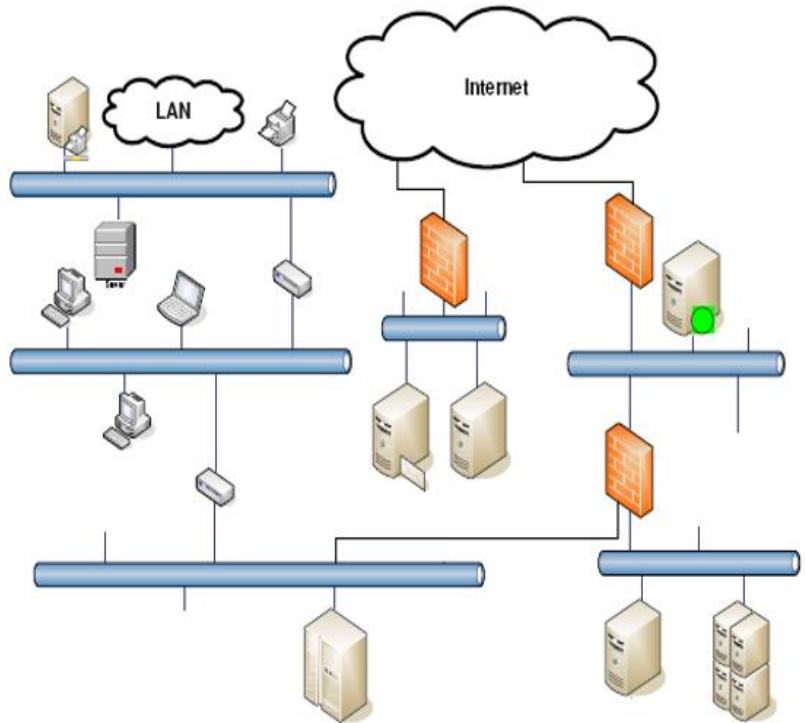
Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584



Know Your Network

Know What “Normal” Looks Like

- Infrastructure
 - Servers & Applications
 - Data Flows
 - Archiving vs. Reviewing
-
- System inventory
 - Application inventory
 - Data inventory



Audit Logs and Password Auditing

- Configure system auditing/logging
 - Understand and document logging capabilities
 - Ensure all systems are configured to log important information
 - Retain logs for at least 1 year, longer is better
- Audit systems for default/weak passwords
 - Most systems have default passwords
 - ◇ Google: “Default password list”
 - Don’t overlook “simple” systems
 - ◇ E.g. Printer/multi-function devices, IP security cameras, etc.
 - ◇ IoT devices...



Action Items

- Review and Validate Your Design
 - Do NOT wait till after you are “in the cloud”
 - Independently validate design
 - Test design BEFORE full production use
 - Periodically test the implemented design
(it changes more often then on-prem systems)

➤ **PRACTICE**

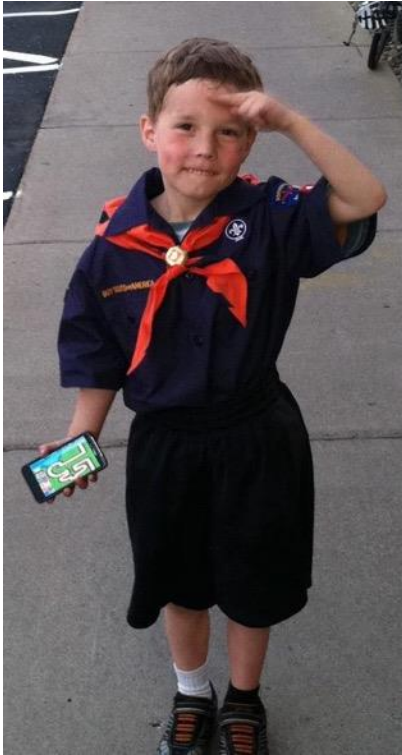


Action Items

- TEST systems and people - Validate that your expectations are being met for cybersecurity
 - Penetration Testing
 - ◇ Collaborative/Informed/White Box
 - ◇ Uninformed/Black Box
 - Social Engineering Testing
 - True Breach Simulation
 - ◇ Red Team/Blue Team

➤ **PRACTICE**





Questions?





Thank you!

Randy Romes

CISSP, CRISC, CISA, MCP, PCI-QSA

Managing Principal – Cybersecurity Team

Direct: 612-397-3114

Randy.Romes@claconnect.com

