Demystifying PCI DSS

Expert Tips and Explanations to Help You Gain PCI DSS Compliance

An eBook by Didier Godart, Risk & Compliance Product Manager at Rapid7

January 2013

RAPID7

Table of Contents

#1 The Basics

Let's start with the basics.

What is PCI?

PCI stands for the **Payment Card Industry**, denoting the debit, credit, pre-paid, e-purse, ATM and POS (Point of Sale) terminal and associated businesses.

But PCI is specifically referring to the Payment Card Industry Security Standards Council (PCI-SSC), a council formed by:

- MasterCard
- Visa
- American Express
- Discover
- JCB

The PCI Council develops and maintains several standards that cover the ecosystem of payment devices, applications, infrastructure and users.

- PCI DSS: (My bible) covers systems that store, process, or transmit cardholder data and is used by acquirers, issuers, merchants, and service providers.
- PCI PTS: covers point-of-interaction devices (or POIs) used for PIN entry.
- PCI PA-DSS: covers payment applications and is used by application developers.

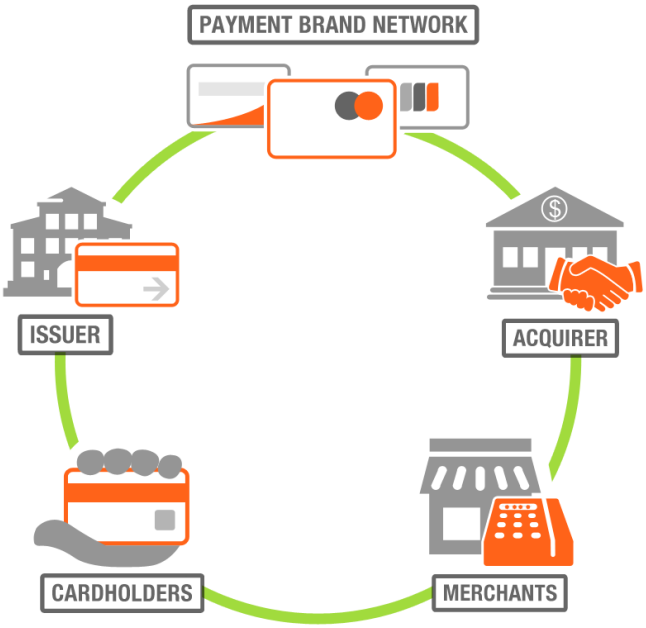
All these standards work together to protect payment transactions and cardholder data.

#2 Payment processing terminology and workflows

One cannot move through the PCI ecosystem without a basic understanding of payment processing terminology and the payment processing workflow. So let's have a look behind the scenes.

Payment processing terminology

In a nutshell, the payment transaction could be depicted as follows:



We have cardholders that make payment card purchases from merchants, merchants that send payment transaction data to their acquirers, and acquirers that send payment transaction data through the payment brand network to the issuer.

- The **cardholder** is the person that actually has the payment card and uses it to purchase goods or services.
- The **merchants** are the organizations accepting payment.
- The **acquirer** is the bank with whom the merchant has a contractual relationship.
- The **issuer** is the organization that issued the card to the cardholder.
- The **payment brands** are the brand of a particular credit card organization, like Visa, MasterCard, American Express, Discover, JCB.

  » Visa and MasterCard will never issue cards. Their cards are always issued through a bank (issuer) or some other organization. American Express, Discover, and JCB International will issue cards directly. They will also acquire those transactions.

Payment processing workflow

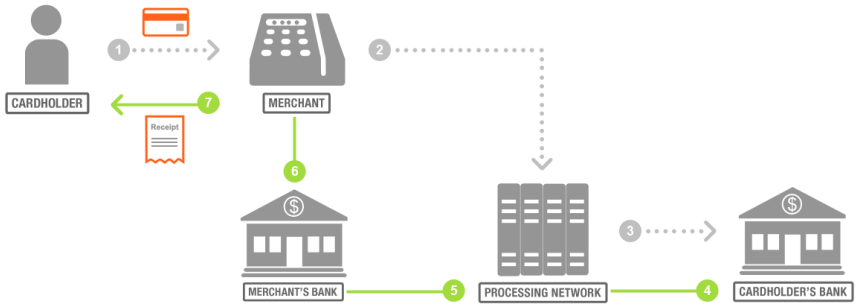
It encompasses the following operations:

1. Authorization
2. Clearing
3. Settlement

Authorization: At the time of purchase, the merchant requests and receives authorization from the issuer to allow the purchase to be conducted, and an authorization code is provided.

The process includes:

1. The cardholder swipes or dips the card at the merchant location.
2. The merchant's bank (or acquirer) asks the processor to determine the cardholder's bank (or issuer).
3. The processing network determines the cardholder's bank and requests approval for purchase.
4. The cardholder's bank approves the purchase.
5. The processor sends approval to merchant's bank.
6. The merchant's bank sends approval to the merchant.
7. The cardholder completes the purchase and receives a receipt.



Clearing: In the Clearing process, the acquirer and issuer need to exchange purchase information to complete the transaction.

The process includes:

1. The merchant's bank sends purchase information to the processor network
2. The processor sends purchase information to the cardholder's bank, which prepares data for the cardholder's statement
3. The processor provides complete reconciliation to the merchant's bank

Settlement: The merchant's bank pays the merchant for the cardholder purchase and the cardholder's bank bills the cardholder.

The process includes:

1. The cardholder's bank sends payment to the processor.
2. The processor's settlement bank sends payment to the merchant's bank.
3. The merchant's bank pays the merchant for cardholder's purchase.
4. The cardholder's bank bills the cardholder.

#3 Distributing the roles for a PCI Play

In this chapter, we'll assign the roles for our PCI Play.

Here's the cast list.

Regulators: Scriptwriters and Directors

They are writing the scenarios and directing the play.

The PCI council whose main responsibilities are to:

- Maintain the standards and supporting documentation
- Qualify assessors and perform quality assurance checks of their work
- Maintain a list of validated payment applications and approved PIN transaction security devices
- Educate the community
- Promote PCI on a global basis

Payment Brands are responsible for:

- Development and enforcement of their own compliance program
- Fines and penalties for non-compliance
- Forensic investigations in case of breaches

Targeted Entities: Lead Actors

They take the lead role by following the director's instructions.

Merchants: Business entities directly involved in the processing, storage, transmission, or switching of transaction data or cardholder data

Service Providers: Same as above but on behalf of merchants.

They must ensure and maintain compliance on an ongoing basis as well as report compliance.

Assessors: Supporting Roles

In this category, the nominees are:

Qualified Security Assessors (QSA): They are qualified by the Council to assess compliance to the PCI DSS standard of merchants and service providers. They go on-site.

List of QSA: https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Approved Scanning Vendors (ASV): They are approved by the Council to perform external vulnerability scans for the targeted entities. To date, there are about 150 approved companies, including **Rapid7**.

List of ASVs: https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

Become an Approved Scanning Vendor (ASV) in 3 Steps: https://community.rapid7.com/community/infosec/blog/2012/02/27/what-you-need-to-do-to-become-an-pci-approved-scanning-vendor-asv

Payment Application Qualified Security Assessors (PA-QSA): They have been qualified by the PCI Council to have their employees assess compliance to the PCI PA-DSS standard. To date, there are 62 qualified companies.

List of PA-QSA: https://www.pcisecuritystandards.org/approved_companies_providers/payment_application_qsas.php

Internal Security Auditors (ISA): Individual security auditor staff of targeted entities qualified by the PCI Council to perform the role of assessor for their organization. Companies using ISA do not need to be assessed by QSA.

PCI Forensic Investigators (PFI): Organizations approved by the Council to investigate the breach cases and verify the level of responsibility of the compromised entity. (See Chapter 18.)

https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

Chapter Notes

Searching for the keyword phrase "PCI compliance" on Google generates more than 9 million hits.

PCI is a business driver for hundreds of security companies that provide a diversity of services to the targeted entities in the preparation and maintenance of their compliance.

#4 Merchant levels: What, Who, and How

In this chapter, I will briefly outline the levels associated with PCI, specifically merchant levels.

What is a level?

A “level” is a classification of organizations accepting and processing credit cards. They are defined and used by the payment brands to indicate what compliance validation procedures and reporting requirements targeted entities are expected to complete.

There is no consensus in this area between payment brands—this would be too easy—so there are as many levels defined as there are payment brands.

They are mainly defined based on the number of transactions processed annually on the payment brand networks.

Who determines the level applicable to a merchant?

Since acquirers are responsible for merchants’ compliance they are the ones who determine the level applicable to a merchant.

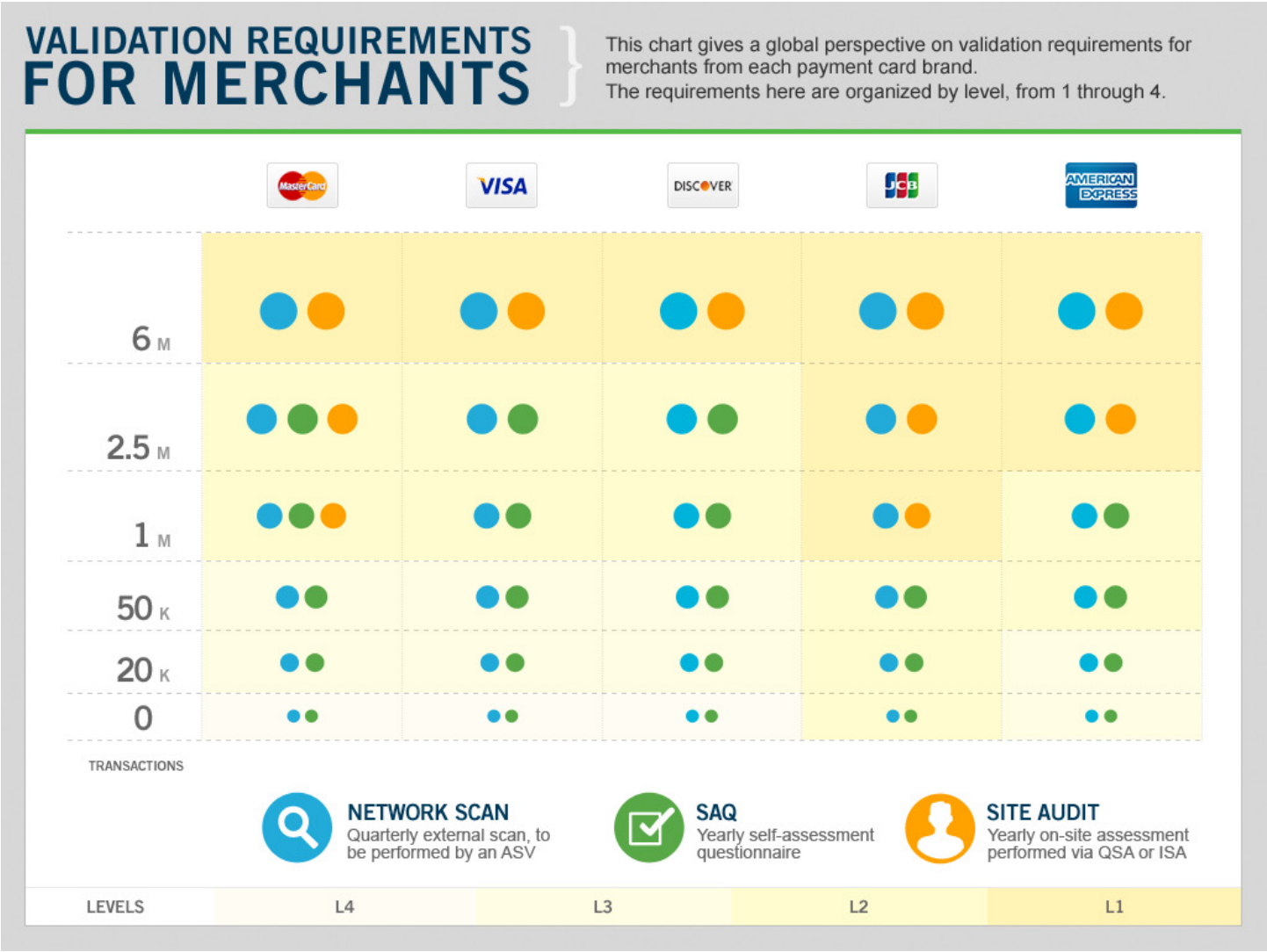
So, if a merchant accepts multiple brands and those brands utilize different acquirers, the merchant could be subjected to multiple levels according to the acquirers.

How do acquirers determine the applicable level?

Acquirers qualify the applicable level mainly based on the number of transactions processed annually, as well as any account compromises experienced by the merchant.

If you are unsure about your level and the validation and reporting requirements application to your company, contact your acquiring bank.

Merchant level definitions by payment brands and transaction volume



Chapter Notes

- No Level 4 merchant for American Express
- No Level 3 and Level 4 merchants for JCB International
- Payment brands reserve the right to escalate a merchant's level dependent on risk such as previous compromise where PCI requirements were not in place.

RAPID7

#5 What's your type?

Do not confused "levels" for "types!"

In Chapter 4, we saw that the payment brands classify organizations that accept and process credit cards by levels. Levels are related to the number of transactions processed annually on the payment brand networks and are used to indicate what compliance validation procedures and reporting requirements targeted entities are expected to complete.

Be careful: do not confuse "levels" for "types," which is another classification used in the context of PCIco.

What's it all about?

If "levels" are associated with the number of transactions processed annually, "types" are associated with the way organizations handle and process cardholder data. They are used to determine which sections and requirements of the PCI bible are applicable to these organizations.

To determine which sections of PCI DSS apply to your organization, you need to know your type.

> » As "types" determine relevant sections and requirements of PCI DSS, they are closely related to the self-assessment questionnaires that organizations are asked to complete as part of the validation procedure.

What are the 5 types?

If "levels" are independently defined by each payment brand, "types" have been defined conjointly by all brands. There are five types namely: A, B, C-VT, C, and D.

	Description
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

Type A: Merchants who do not store cardholder data in electronic form and do not process or transmit any cardholder data on their systems or premises.

Type B: Merchants who process cardholder data only via imprint machines or standalone, dial-out terminals.

Type C-VT: Merchants who process cardholder data only via isolated virtual terminals on personal computers connected to the Internet.

Type C: Merchants whose payment application systems are connected to the Internet.

Type D: All other merchants who do not meet the above descriptions.

If you are unsure about your type, ask your acquiring company.

References

For more information about how to determine your type, please review the PCI Data Security Standard Self-Assessment Questionnaire.

#6 The Validation Toolbox

PCI is probably one of the few compliance programs out there equipped with a compliance validation toolbox. In this chapter I would like to briefly cover the content of this toolbox.

ASV network vulnerability scans

This tool has been specifically designed to help organizations meeting one particular requirement of PCI DSS (11.2.2).

> "Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC)."

PCI requires the external network scans to be performed by security companies qualified by PCIco on an annual basis (Approved Scanning Vendors).

The scope of the external vulnerability scan must include all externally accessible system components that are part of the cardholder data environment. It should also include any externally-facing component that provides a path to the cardholder data environment.

The scan customer is responsible for defining the scope of the external vulnerability scan. If an account data compromise occurs via an externally facing system component not included in the scan, the scan customer is responsible. For more information on the CDE Scope, see Chapter 9: Defining the Scope of the PCI assessment.

ASVs are to validate any IP addresses found during the scan with the scan customer to determine whether or not they should be included within the scope of the assessment.

ASV scan report consists in three parts:

- An attestation of compliance (AOC) (global compliance attestation)
- An executive summary (component compliance summary information)
- A detailed vulnerability report (detailed list of vulnerabilities)

Notes:

- A passing result is obtained when the scan report does not contain any high or medium severity vulnerabilities, as well as no automatic failures as defined byPCIco
- To be considered compliant an organization must pass four consecutive ASV scans within twelve months

Find out what to do if your organization can't demonstrate four passing PCI internal or external scans: https://community.rapid7.com/community/infosec/blog/2011/09/22/what-to-do-if-my-organization-can-t-demonstrate-four-passing-pci-internal-or-external-scans.

Self-assessment

The self-assessment questionnaire (**SAQ)** allows organizations to self-evaluate their compliance with PCI DSS. This is a useful tool to determine, document and follow up alignment with the standard. Actually, there is a specific SAQ version for each merchant "type" (see Chapter 5). Each SAQ covers only PCI sections and requirements relevant to the corresponding merchant type.

The SAQ consists of two parts:

1. Questions correlating to the PCI DSS requirements
2. Attestation of Compliance (AOC) or self-certification that a company is eligible to complete a specific SAQ type

The different SAQ versions were originally designed to be filled out by hand and were only available in PDF format; however, the current official edition is available in both PDF and Word format. In addition to these official formats, I currently maintain an Excel version that combines all the self-assessment types into one sheet (see the "PCI Compliance Dashboard" in References). In addition, there are online SAQs platforms available that facilitate completion of your self-assessment.

On-site audit

This tool is a thorough assessment performed within organizations to validate their adherence to the standard. Such assessments must be conducted by qualified external (QSAs) or internal security auditors (ISAs) trained and approved by PCIco.

If internal individuals are used, they must belong to an internal audit organization. For obvious independence reasons, IT staff or information security staff could not perform the assessment.

On-site audit includes:

1. Validation of the scope of the cardholder data environment
2. Verification of all technical and procedural documentation
3. Confirmation that every PCI DSS requirement has been met
4. Evaluation and acceptance or rejection of compensating controls
5. Production of the Report on Compliance (ROC)

References

- PCI reference page about PCI assessors (QSAs, ASVs,ISAs)
- SAQs instruction and guidelines
- PCI Compliance Dashboard
- Mastercard PCI validation requirements
- Visa validation requirements
- Amex validation requirements
- JBC validation requirements

Which tools are relevant for my organization?

If the validation rules are specific to each payment brand, they are all based on the merchant "levels" (see Chapter 4).

Depending on your level you will either need to go through an annual on-site audit or complete the SAQ appropriate to your type (Chapter 5). It is highly recommended that entities that conduct an annual on-site audit also complete the SAQ as a preparation for the on-site inspection.

» The best way to know what validation tools you are subjected to is to refer to your acquirer(s).

» VISA Canada is requiring Level 2 and 3 merchants to validate their SAQs with a QSA. Personally I don't see any QSA endorsing a SAQ without a thorough inspection so I don't see any difference between this validation and an on-site audit, particularly in terms of cost for the entities subjected to compliance.

#7 Certification programs, striving for quality

In 2005—for the first time in history—all major payment brands collaborated together to create a unique set of requirements (PCI DSS) aimed at reducing credit card fraud. As a consequence, we have seen a demand for new security-related solutions and services emerging.

We didn't have to wait long to see the security industry respond to this demand, integrating the three letter acronym into their marketing plans. Suddenly every security company is a self-proclaimed PCI expert and is offering to help you become compliant. With so much noise, there was a need for some kind of regulation to guarantee the quality of all this 'help.' The PCIco partly addressed this need by establishing the thresholds for qualification of two major actors of the program: namely the Approved Scanning Vendors (ASV) and the Qualified Security Auditors (QSA).

I was working at MasterCard in 2005 when the requirements were put together and was personally charged with the creation and management of the certification program for ASVs. The PCIco does not certify products; this is not their core competency and never will be, so the aim of the ASV certification is to verify the ability of a scanning vendor to detect, report vulnerabilities and misconfigurations.

My team had to do something that had never been done: build an *intentionally* insecure network. While this sounds fairly easy—by definition, isn't it insecure out of the box? However, it's actually not straightforward to do it deliberately for a heterogeneous network of firewalls, routers, DNS, mail, application and database servers comprised of a diversity of services and applications. Furthermore, we had to know the exact list of flaws for each target. We did this to replicate the process ASVs go through when they scan a network.

Without much more information than a list of IPs, vendors have to scan 10-16 remote targets within a specific time window, which may be considered too short for some of them. Vendors are expected to treat the certification body (test lab) as a customer, using the same process and scanning technology they intend to use on the field.

Having led this program for about 5 years, I can tell you how difficult it is to pass the test. Targets are regularly reconfigured and vulnerabilities frequently added or removed.

To pass the test, a vendor must report their results in the expected PCI format and reach a specific threshold (%) of findings for each target.

I saw hundreds of companies fail again and again, while others passed, with our compliments, each year. I came to the conclusion that the success resides in two areas:

1. The scanning technology used—made of up of a scanning engine, vulnerability databases, and reporting systems.
2. The skills and knowledge of individuals using the scanners—while not all scanners are adequate for the task, scanners that have been incorrectly configured are disastrous.

Since April 2011, the PCIco has been pushing their quest for quality by requiring employees of ASVs to take training and pass a test on an annual basis, in addition to the existing requirement for the organizations ASV solution to be annually recertified. Furthermore, the PCIco is currently defining a quality program with the aim of controlling ASVs on the field.

Much more still needs to be done in the domain of quality and qualification though. One area where we could see the PCIco adopting a certification program in the future is penetration testing, though at present this is occupying a kind of no man's land for ambiguous reasons.

#8 DSS in a nutshell

PCI DSS was originally developed by MasterCard and Visa through an alignment of security requirements contained in their respective programs to secure ecommerce: the Site Data Protection for MasterCard and the Cardholder Information Security Plan (CISP) for VISA US.

PCI DSS adopts a top-down approach. It starts with six high level goals. This terminology is confusing because the unique goal of the program is to protect cardholder data while transmitted, processed, and stored by an entity. (Instead of "goals," I would prefer to call them "sections" or "domains.") Those goals are then mapped against 12 requirements that each subdivide into more granular requirements. Each requirement comes with a set of corresponding testing procedures.

So thinking that PCI DSS compliance is just about implementing 12 requirements is inaccurate. In reality, there are more than 200 specific requirements.

This graph depicts the combination of the two first layers of requirements:

The six goals, sections or domains are:

G1: Build and maintain a secure network

G2: Protect cardholder data

G3: Maintain a vulnerability management program

G4: Implement strong access control

G5: Regularly monitor and test networks

G6: Maintain an information security policy

The 12 high-level requirements are:

R1: Install and maintain a firewall configuration to protect cardholder data

R2: Don't use vendor-supplied defaults for system passwords and other security parameters

R3: Protect stored cardholder data

R4: Encrypt transmission of cardholder data across open, public networks

R5: Use and regularly update anti-virus software

R6: Develop and maintain secure systems and applications

R7: Restrict access to cardholder data by business need-to-know

R8: Assign a unique ID to each person with computer access

R9: Restrict physical access to cardholder data

R10: Track and monitor all access to network resources and cardholder data

References

The PCI DSS V2: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PCI Compliance Dashboard: https://community.rapid7.com/docs/DOC-1512

R11: Regularly test security systems and processes

R12: Maintain a policy that addresses information security

» Why 6 domains and 12 requirements? Actually the MasterCard SDP and Visa CISP programs consisted respectively of 12 and 6 requirements. As both wanted to keep their numbering they reached a compromise. So the current structure of the PCI DSS is the end result of a compromise.

» Are all requirements relevant for my organization? No, the relevance of requirements for your organization depends on your "type" (see Chapter 5).

#9 Defining the Scope of the PCI assessment

Entities subjected to the PCI program have the ultimate responsibility for defining the scope of the PCI assessment.

According to the rules, the PCI scope must encompass all "system components" included in, or connected to, the Cardholder Data Environment (CDE).

What is the CDE?

The PCIco defines the Cardholder Data Environment as the people, processes and system components that store, process or transmit cardholder data or sensitive authentication data.

> » There is a simple way to understand the difference between cardholder data and the sensitive authentication data. The cardholder data is displayed on the front side of your credit card, such as the full PAN, cardholder name, and expiration date. The sensitive authentication data is generally printed on the back and is used to authenticate cardholders and/or authorize payment card transactions, such as card validation codes and full magnetic-stripe data.

What are system components and what do they mean?

Let's be clear on what we mean by system components:

- Network components such as firewalls, switches, routers, wireless access points, network appliances and other security appliances.
- Servers such as web, database, authentication, mail, proxy, time synchronization, and domain name.
- Applications, purchased and custom applications.

I would also add the component of *people* into the business departments that deal with cardholder data, as well as any departments associated with the management, security, installation and maintenance of the above system components.

How do you determine the scope?

The scope of PCI compliance can be extremely difficult to determine. One of the best ways to handle this critical exercise is by adopting a top-down approach through two series of workshops.

The aim of the first workshop is to capture the entire end-to-end business process, understand where cardholder data is used and for which purposes, and identify third party relationships and dependencies. The second workshop should be much more focused on technical aspects, such as the identification of system components and technical procedures that support the business' processes.

The final exercise in scoping is to create the scope document, which details what is in and what is out of scope of PCI compliance, as well as the rationale behind these findings. This document should be regularly reviewed. The **PCI Compliance Dashboard** can help you in documenting and maintaining your scope.

How do you reduce the scope?

The scope of a PCI assessment could reveal quite large for some organizations and therefore quite demanding in terms of resources, time, finance—as well as being an considerable source of stress. To minimize these considerations, the associated expenses, and the risk of non-compliance, it's of the utmost importance for entities subjected to PCI compliance to reduce the scope as much as possible.

To do so, one may consider the following areas:

1. Reducing the need for data storage

Ask yourself the following question: Do we *really* need to keep cardholder data? Minimizing where card data is stored helps to reduce the scope.

2. Network segmentation

Network segmentation consisting in isolating the cardholder data environment from the rest of the organization's data is perhaps the best way to limit scope.

At a minimum, segregation should entail logical separation between networks via router and switch ACLs, as well as involving the separation provided by a firewall. The optimal solution being the physical separation between networks.

> » PCI defers to the QSA (for organizations subjected to on-site audits) to render judgment about what is acceptable in terms of network segregation. Different PCI QSAs interpret this differently, adding to the challenge of PCI compliance.

For those not subjected to on-site audits, the acceptable level of segregation is left to their own judgment.

3. The use of third party solutions

In many cases entities are storing cardholder data unnecessary. The most common reasons cited for this are recurring billing and dealing with chargeback or disputes.

Outsourcing this data storage to PCI-compliant service providers that can securely manage your payment processing and securely store your records is definitely a way to reduce the scope of the assessment. There are a lot of third party solutions available that will store and perform the necessary financial operations - authorization, clearing and settlement - on your behalf. Such solutions usually use tokenization to help you deal with recurring payment. Tokenization allows you to replace the PAN with a less sensitive token in your database. For more information, see Chapter 11.

Dealing with chargeback and disputes (the return of funds to a consumer, forcibly initiated by the consumer's issuing bank) does not require the full PAN but generally only the last four digits. So you could reduce the scope via that mechanism as well.

> » Speak to your acquirer or processors to know what they would need from your organization to handle chargeback and disputes.

> » Keep in mind that outsourcing payment processing and data storage does not absolve an entity from the responsibility to process payments on behalf of the business in a PCI-compliant fashion. The merchant or business still owns and is responsible for meeting this requirement regardless of whether or not these processes are outsourced.

#10 The Prioritized Approach

As introduced in Chapter 8, organizations subjected to compliance are required to implement more than 200 requirements. With this in mind, achieving compliance can be a painful, long, and costly exercise, so one might wonder how best to approach this daunting task. In response, the PCIco shared their view on the best approach to compliance. They code-named this the "Prioritized Approach."

What is it?

A tool to help and guide organizations establish a roadmap for compliance, and demonstrate progress to key stakeholders.

Who is it for?

The prioritized approach is suitable for merchants who undergo an on-site assessment or use self-assessment type D (see Chapter 5).

How does it work?

Any roadmap is composed of milestones. The prioritized approach suggests dividing compliance projects into six phases, each of them targeting specific security controls laid out in the standard:

1. **Remove sensitive authentication data and limit data retention.**

   Scope reduction (see Chapter 9), data retention and disposal, destruction of unnecessary data.

2. **Protect the perimeter, internal, and wireless networks.**

   Traffic control, firewall, routers, DMZ, logical and physical access control, line encryption, IDS, internal and external scanning, penetration testing.

3. **Secure payment card applications.**

   Hardening, standard configuration, patching, secure coding practices and procedures, Web scanning, application firewall.

4. **Monitor and control access to your systems.**

   Access management, users identification and authentication, user activity monitoring and audit trail, WAP monitoring, file integrity monitoring, incident response.

5. **Protect stored cardholder data.**

   Data encryption and masking, key protection and management, backup media handling, visitor handling.

6. **Finalize remaining compliance efforts and ensure all controls are in place.**

   Policies, procedures and standards not covered above.

The PCI DSS Compliance Dashboard Tool

The tool is actually a spreadsheet listing all PCI DSS requirements together with their associated milestones. Multiple columns such as compliance status, stage of implementation, estimated date for completion and two graphs help tracking progress toward compliance.

References

- Prioritized Approach for PCI DSS Version 2.0
- PCI Compliance Dashboard

#11 Tokenization

Chapter 9 introduced "tokenization" as one acceptable technique to reduce the scope of the cardholder data environment or CDE. Let's clarify this concept in this chapter.

The Concept

The concept of tokenization is quite simple to understand: replacing a valuable asset with a non-valuable one. This is the same principle as when a museum uses replicas for public exhibition while keeping authentic artworks secure in its safe, or how a casino uses tokens while keeping cash secured in the vault, or when you leave your coat in a cloakroom in exchange for a ticket.

Tokenization for PCI: Killing two birds with one stone

Here, the valuable asset is the cardholder data, and more specifically the PAN (Primary Account Number: the credit card number also known as account number). Tokenization consists of swapping PANs wherever they are stored by a piece of information (token) that will be not be attractive for criminals since the token can't be used for transactions or fraudulent charges, so there is little harm done if it's stolen. PANs could then be eliminated or stored for further reference in an electronic vault located internally or externally.

The notion of tokenization within the PCI framework was originally introduced in DSS v2.0 as an acceptable solution to comply with requirement 3.4:

> "Render PAN unreadable anywhere it is stored (including on portable digital media, backup media and in logs)."

But we didn't have to wait long to see it used in the context of 3.1:

> "Keep cardholder data storage to a minimum."

Hence: Killing two birds with one stone.

The Downside

As tokens are replacing the sensitive PANs, any components processing or storing this information could be removed from the scope. The downside is that all elements of the tokenization system - including the PAN vault and any system component or process with access to the tokenization system - must be considered an important part of the CDE and therefore in scope for PCI compliance.

Additionally, one should not overlook the effort and cost related to the selection of an appropriate solution supporting all their platforms as well as the effort and cost of implementation of such a solution in their environment.

Guidance and regulations

The council quickly understood the urgency of establishing guidance and regulation in this area. The result is available in the council library under the title: "PCI Tokenization Guidelines."

References

PCI Tokenization Guidelines

#12 Mind The Gap

Once the scope of the assessment is determined, our next stop on the PCI roadmap is the gap analysis process.

Objective

Identify gaps between where we stand and where we want (or need) to be in terms of compliance. This process provides a foundation for measuring the investment of time, money and human resources that's required to achieve a particular outcome; in this case, PCI compliance.

Who should perform a gap analysis?

Though there is no obligation to perform such an analysis, I would recommend that all entities subjected to compliance perform this exercise regardless of their level or type. For those subjected to on-site audits it will efficiently prepare you for the QSA visit. For others, it will sustain the self-assessment process. In both cases, it could be driven either internally or through the expert eyes of external parties.

How long does it take to perform a gap analysis?

Don't underestimate it! A gap analysis process could last between a few days to several months, depending upon the scope, the level of control of the environment—meaning the internal business and technical knowledge and expertise—and finally, the level of understanding of PCI DSS. I would also consider the attitude and open-mindedness of participants.

The process

A gap analysis process should encompass the following actions:

- Identify the DSS requirements pertaining to the entities (merchant "types").
- Identify the actors: individuals sharing business or technical expertise of the environment and who should take part to the exercise.
- Determine compliance status: discuss the compliance status of each component in scope against relevant requirements through brainstorming sessions and interviews with the actors.
- Document the rationale for compliance; don't limit yourself to a "Yes," justify in detail why, in your opinion, you meet compliance. Attach proofs of compliance. Describe compensating controls.
- Identify ambiguous areas to be further investigated with the assistance of the community or experts.
- Identify areas of non-compliance and develop remediation plans.
- Prioritize the gaps and define a timeline for achieving compliance and assign ownership.

Outcome

I generally see the outcome of a gap analysis as a compliance dashboard, which provides us with a global view on:

- Areas of compliance and associated proofs.
- Areas of non-compliance associated to remediation plans, timeline and ownership.

Tool – PCI DSS Compliance Dashboard

Please feel free to use this Compliance Dashboard spreadsheet to sustain your gap analysis exercise. It encompasses:

- A table of content and navigation links
- Add "Scope" sheet allowing you to define the Card Data Environment (CDE)
- An executive summary showing your progress on your PCI compliance journey based on the selected merchant type
- Add two buttons within the Executive Summary Sheet allowing you to hide/unhide non applicable requirements associated to the selected Merchant Type.
- Graphs (Compliance % and Severity Level per requirements
- All PCI DSS requirements grouped by section
- Guidance associated to each requirements
- The major observation points from the 2011 Verizon PCI Compliance report for each requirement
- The PCI Glossary
- The participants list ("PCI Team")
- The list of merchant types
- The compensating controls documentation sheet
- The Validation Instructions for QSA/ISA for each requirement
- Indication of "relevance" by merchant types (A, B, C, C-VT, D). "1" indicates that the requirement is relevant.
- Priority level or milestones from the "prioritized approach" (1-6)
- A column "In Place" (Yes/No/Compensating control Present)
- A column severity equals to the PCIco priority level for not in place requirements
- A column "Stage of implementation (if not in place)"
- A column "Estimated date for completion"
- A column "Proofs/Documentation/Comment"
- A column "Remediation plan" (what must be done)
- A column "Owner" (The individualor department in charge)
- A column "SANS Top 20 Critical Security Controls" matching subcontrols for each PCI requirement wherever possible. (NEW)
- A sheet "SANS-PCI" Listing all SANS Top 20 Critical Security Controls and Sub-controls together with PCI requirements partially or fully matching the sub-controls. Also a % of match for each SANS Controls.

Want to give it a try? Download your customizable PCI Compliance Dashboard.

#13 Compensating Controls: Magic Trick or Mirage?

There are circumstances where companies could face some technical or business impediments preventing them from implementing the requirements as explicitly stated in the PCI standard.

Does this mean that these companies could never achieve and maintain compliance?

There is a common misconception that organizations must meet the requirements as they are written. This is not the case. The important thing is that the inherent security objectives behind each requirement are met. The PCIco and the Payment Brands provide some flexibility by allowing companies to pull a rabbit out of their hat. This rabbit is named *compensating controls*: a very popular topic these days as more and more organizations look at it as a way to achieve compliance. But is this really the case?

What is a compensating control?

A compensating control is a work-around for a security requirement. In other words: it's another way to reach the objective sustained by a specific security requirement without satisfying the requirement itself. Understanding this requirement and its objective is therefore of the utmost importance in choosing and evaluating a compensating control.

You can refer to "Navigating PCI DSS" to get an understanding of the objectives behind each requirement.

For which requirements should compensating controls be used?

With the exception of requirement 3.2—Do not store sensitive authentication data after authorization—any security objectives supported by the PCI DSS requirements can be met with compensating controls.

There is, however, a caveat to the above statement. Companies must prove that the roadblock to implementing the requirement is temporary and due to "legitimate" technical or business constraints. The term "temporary" is important as the situation must be reviewed on an annual basis.

What does "legitimate" mean to the Council? It isn't very explicit on this. Definitely the cost of implementation isn't a legitimate constraint for them, but an application running on an old non-supported operating system (sustained by a migration roadmap) or the Christmas sale load delaying implementation are two examples of acceptable legitimate constraints provided by the Council at the 2011 PCI community meeting.

What is a valid compensating control?

To potentially be considered valid, a compensating control must fulfill the same intent and objective of the requirement it's supposed to replace, with the same or higher level of defense, and without introducing any other risks (border effects) or with any additional risks both minimized and documented.

So, the root of the issue is whether or not the risks have been sufficiently addressed: Both the risk of not implementing the requirement and the risk inherent to the selection of the compensating control.

How do you document a compensating control?

Every compensating control must be supported by a risk analysis and must be documented as follows:

- What is the original objective that one tries to cover?
- What are the legitimate constraints preventing meeting the original requirement?
- What is the compensating control?
- What are the identified risks posed by the lack of original control or introduced by the implementation of the compensating control?
- Who should validate a compensating control?

According to the standard, QSAs are the ones responsible for validating the compensating controls, at least for Level 1 merchants and service providers. There are no other validators than the acquirers themselves for all other merchant levels.

However, the majority of the QSAs are NOT in favor of compensating controls and would dissuade their customers from using them. According to them, compensating controls could reveal themselves to be much more costly and difficult to implement than the requirements they replace. The fact that QSAs must sign off the compensating controls is probably another reason for this reluctance.

Additionally, there is no unification for the validation of the legitimate constraints and compensating controls among QSAs. A compensating control could be seen validated by one QSA while being rejected by another.

A central database of “historically accepted compensating controls and legitimate business or technical constraints” could be of some added value for the community.

Conclusion

My interviews with the Council, the Brands and the QSAs on that matter leads me to conclude that due to the stringent constraints imposed by the PCIco on the selection and use of compensating controls, combined with the QSAs reluctance to approve the use of compensating controls, and also the lack of unification, compensating controls should be considered more as a mirage than a magic trick.

References

Navigating PCI DSS

#14 The World Isn't Perfect

According to the 2011 Verizon Payment Card Industry Compliance Report, requirement 11—Regularly test security systems and processes—is the one least met, so I thought I would dedicate a few chapters to this subject, starting with the definition and source of vulnerabilities.

The term "vulnerabilities" is often used in the PCI DSS standard to mean the following (per the definition given by the Council):

> Flaws or weaknesses which, if exploited, may result in an intentional or unintentional compromise of a system.

Let's illustrate this by taking our body and soul as the system.

Examples:

As a first example, imagine that I'm standing in front of you holding in my hand a test tube containing an explosive product. I warn you to move carefully because this product is movement sensitive. Ah, I can see the fear in your eyes! Suddenly I shake my hand...nothing happens. I explain to you that for this product to be so reactive one needs to add a drop of a reagent.

Now let's imagine that while I'm talking to you someone does so behind my back. What would have happened if I shook the test tube? Yes, indeed—sorry, it wasn't my fault!

As a second example, let's analyze the following scenario: A car fatally hits you while you are quietly crossing the street. Here you are the system. What could have caused this awful scenario? Bad luck maybe? There are multiple factors that could have lead to this scenario. You simply crossed without paying attention: you had your iPod on; the car driver didn't see you; you had a bad day and you were deep in thought; you are blind, deaf, or both. The environment is also playing a role: Crossing a city boulevard during the peak hours is quite different to crossing a country street on a Sunday morning.

The factors above are the weaknesses or vulnerabilities that increase the probability of occurrence of this scenario.

Vulnerabilities in information systems

The world isn't perfect and certainly the world of information technology is no exception. There are a variety of vulnerabilities across information systems—including computers, network systems, operating systems, and software applications—that may originated from vendors, system administration activities, or user activities:

> Vendor-originated: this includes software bugs, vulnerable services, insecure default configurations, and web application vulnerabilities.
>
> System administration-originated: this includes incorrect or unauthorized system configuration changes, lack of password protection policies.
>
> User-originated: this includes sharing directories, opening infected documents, selecting easy guessing password, downloading and installing third party software.

Why aren't bugs fixed before software release?

Bugs are a consequence of the nature of human factors in the programming task. They arise from oversights or mutual misunderstandings made by a software team during specification, design, coding, data entry and documentation.

As computer programs grow more complex, bugs become more common and difficult to fix. Often programmers spend more time and effort finding and fixing bugs than writing new code support. On some projects, more resources can be spent on testing than in developing the program.

There are various reasons for not fixing bugs:

- The developers often don't have time or it is not economical to fix all non-severe bugs.
- The bug could be fixed in a new version.
- The changes to the code required to fix the bug could be large, expensive, or delay finishing the project.
- Even seemingly simple fixes bring the chance of introducing new unknown bugs into the system.
- "It's not a bug." A misunderstanding has arisen between expected and provided behavior.

Given the above, it is often considered impossible to write completely bug-free software of any real complexity. As a consequence software is released with known or unknown bugs.

Is it a problem? Well, let's see in the next chapter.

#15 Nice Look!

In the previous chapter, we discussed why bugs aren't fixed in software before release.

Once software is released and installed within our environment these weaknesses are on our side. Is it a problem?

Some examples:

Let's take the image of a bridge, a strong and proud bridge. Cars are driving through it the whole day without being aware of the presence of a weakness in its internal structure. In appearance, no threat, no risk. And then there is a fateful day when an earthquake intensively shakes the city. While the bridge was supposed to resist this intensity, it failed and collapsed, sweeping along a dozen cars and their passengers into the river.

A sudden tragedy revealed the hidden threat. Of course, if people would have known about the weakness they would probably assess the associated risk and block the bridge, right? Well, I'm not sure because taking such a decision would have had a huge impact for the city. This is related to the decision process.

Let's take a second example.

Imagine that you stand in a humid swamp infected by mosquitoes and that you are allergic to their bites. Fortunately your entire body is sheltered under your special gear. However, you didn't notice a tiny tear in your gear—tiny, but big enough to let a mosquito bite you. The consequence will depend of how much you are allergic to mosquito bites. The merchant you bought it from would not replace your gear, but suggests you sew it up or stick on a small piece of material to patch the hole.

The consequences of software bugs in our environment

The presence of software bugs or holes within our environment could create a whole set of issues such as preventing legitimate users from accessing functionalities; impacting the performance and usability; crashing services or servers; leading to confidentiality breaches; escalating user privileges; soiling data integrity. Is this a problem? Well, it depends of the severity of the bugs (what the bug could lead to) and the criticality of the environment on which they run.

The same bug could reside simultaneously on a production server and a test server. The same bugs will have the same consequence on both servers such as leading to crashes, but the criticality would be more important for the production server than the test server. This aspect is of the utmost importance when considering a remediation plan. But before fixing a bug, one must detect it.

As said in Chapter 14, bugs could be known or unknown. They could be detected accidentally or through code analysis and application testing. They could be detected by company developers or testers, by the users or by malicious individuals looking for them. Once known they should be fixed. This fix generally consists in writing a small piece of software called a "patch" in the same way the merchant or tailor would apply a patch on your gear.

I'll let you decide how you would look if your clothes consisted of as many holes as there are in software. Maybe this could become a new fashion.

Once bugs are detected and fixed on the software company side, they still need to be fixed within our environment, and that's another story.

RAPID7

#16 Is your organization behaving like a fashion victim or a clown?

In the last chapter, we discussed the severity of the presence of bugs in software, and how these bugs are handled on the software vendor's side. Now, let's discuss the customer organization's side.

What can we do about software defects?

Software is buggy. This is a fact (see Chapter 14). Returning to the analogy of protection gear, my son is constantly reminding me that wearing pants with rips and holes is actually the fashion and I should accept it. Personally, I find it quite weird that the price of a piece of clothing increases with the number of scratches and holes in it.

Similarly organizations are facing a crucial dilemma: Either leave holes in software and look like a fashion victim or wear so many patches you look like a clown. Not a great choice. The solution is somewhere in between.

The problem is that, as we discussed in our last newsletter, holes equal vulnerabilities, which equal risk for the organization. The whole process of reducing risks associated with holes in software is called vulnerability management, a strange denomination as a vulnerability could be more than a simple hole in the cloth, I mean in software. I would prefer to call this process "the holes and defects quest."

Vulnerability management plays a major part in the workload of individuals responsible for security. It is highlighted by all best practices and guidance manuals, as well as by all regulations and compliance programs, including the sixth and seventh verses of the Data Security Standard bible:

§6: You will develop and maintain secure systems and applications

§11: You will regularly test security systems and processes.

What is involved in a vulnerability management program?

The medical world follows a specific protocol to cure patients:

- Diagnose: Identify the patient's illness based on symptoms and a panel of test results.
- Determine the risk: What could the impact be for the patient if the illness is not cured?
- Prescribe: Determine what remedy could be applied, if any, and the potential side effects for the patient.
- Decide: Based on the above data, the doctors and the patient decide on a treatment plan.
- Treatment: The patient applies the prescription.
- Control: The doctors perform regular checks to make sure the cure is on working as expected.

Curing software of vendor vulnerabilities (holes, defects) follows the same protocol.

- Diagnose: Identify the presence of (known) holes/defects (vulnerabilities) through a set of tests called network/system/application/database scans.
- Determine the risks: Assign a risk level to each identified vulnerability accounting for the consequences of security incidents from exploiting the vulnerability, the existence of scripts (exploits) facilitating the exploitation, the nature/sensitivity of the organization, the presence of compensating controls reducing the exploit intensity, the time elapsed since the vulnerability exposure and the existence of remedies. Penetration testing is a useful tool to help you quantify the real level of risk associated with the identified vulnerabilities.
- Prescribe: List all countermeasures leading to remediation or risk mitigation as well as the additional risks (side effects) induced by the application of these remedies.
- Decide: Based on the above information, determine prioritization and the more appropriate action plan, assign responsibilities.
- Treatment: Follow action plan.
- Control: Verify the effectiveness of the action plan through regular checks (scans)

#17 Why are my scan reports so thick? - Impact of "potential" vulnerabilities

"My PCI scan report has more pages than the NASA report related to the crash of the space shuttle Columbia."

This acerbic statement was made by a merchant complaining about the size of his external scan reports.

Verse #11.2 of the PCI data security bible requires organizations subjected to PCI compliance to run internal and external network vulnerability scans at least quarterly on their CDE (card data environment). The PCIco regards risk relating to the internal and external sides of the CDE differently. This translates in the subdivision of verse 11.2 into §11.2.1 (related to internal scanning) and §11.2.2 (related to external scanning). While the level of flexibility and initiative allocated to companies is indecently large in terms of internal scanning—where organizations may basically do whatever they want—external scanning is subject to more demanding, structured, and explicit rules, starting with the mandated use of an approved scanning vendor (ASV) submitted to annual certification. When running scans, ASVs must strictly comply with specific rules published by the PCIco in a document called: ASV Program Guide Reference.

Why are external scanning reports so thick?

The major causes of the thickness of a PCI scan report are:

1. The extent of the scan fields.

It wouldn't surprise anyone to state that the more targets you have to scan, the thicker your report would be.

2. The structure of the scan report

As part of the ASV Program Guide, the PCIco requires ASVs to report scan results in a specific way. The report must consist in threefold:

a) A short attestation of compliance
b) An executive summary
c) A detailed vulnerability report

In terms of structure, the pain part is the executive summary that is far away from being what one would expect from an executive summary: short and straight to the point. The PCIco requires the executive summary to list all detected vulnerabilities for each target, including the severity level, the CVSS score, the compliance status (PASS or FAIL) as well as any associated exception, false positive or compensating control. Additionally PCIco requires that the long executive summary be amended with a consolidated solution/correction plan for each target.

Based on the above, one could easily understand why an executive summary would be long. Hopefully, one could expect in the near future a new version of the ASV Program guide, wherein the executive summary would be split into a real executive summary and a technical summary limited to the list of detected vulnerabilities that do not pass the compliance threshold in terms of severity and excluding informational results. Those are the ASV's recommendations made in 2010 to PCIco.

3. Potential vulnerabilities

Many merchants ignore what a "potential vulnerability" is and show suspicion when being told by their ASV about it, as this term is absent from the PCI glossary and PCI DSS bible. However, potential vulnerabilities weight highly into the causes of the report thickness as well as into the causes of scan failure and workload associated with the vulnerability management.

The PCIco introduces this term into the ASV Program Guide as a "vulnerability from which the presence cannot be determined with certainty." Unfortunately nothing is said about what the PCIco considers as "certainty."

Abstract—ASV Program Guide V1, page 14:

> In addition to confirmed vulnerabilities, ASVs must report all occurrences of vulnerabilities that have a reasonable level of identification certainty. When the presence of a vulnerability cannot be determined with certainty, the potential vulnerability must be reported as such. Potential vulnerabilities must be scored the same as confirmed vulnerabilities and must have the same effects on compliance determination.

Confirmed versus potential?

For a neophyte, it could sound strange to say that an ASV could be "uncertain" of the presence of a vulnerability. Why is that?

The root of the answer lies in the "blind" nature of an external scan. Scans are performed remotely through the Internet with no privileged (admin) access to the targets as this would require transmitting admin credentials through the Internet, which is not a recommended practice. Furthermore, the signature (name and version) of the targets could have been voluntarily modified or obfuscated for the sake of security.

In the same way SONAR recognizes boats based on the noise pattern generated by their engines, some vulnerabilities could be determined with a high level of certainty based on the response patterns received from targets. Another bunch of vulnerabilities are reported only because such service name, such version number and patch levels have been (maybe erroneously) determined. Those latest ones are what the PCIco considers potential vulnerabilities. However, for the readers of a scan report there is no difference between confirmed vulnerabilities and potential ones. They are all falling into the long list of reported vulnerabilities.

Besides impacting the size of the scan report, potential vulnerabilities are causing a high rate of false positives and therefore impacting the reliability of the scan results and the workload of the individuals in charge of verifying the level of certainty of each vulnerability. They are not considered to add value by many ASVs. In fact, some ASVs go so far as to play against the rules by completely ignoring them from their scan reports in order to increase the level of accuracy of their reports and customer satisfaction.

Despite their evident low added value and poor impact on the accuracy of the scans, the thickness of the reports and the workload, the PCIco persists in requiring ASVs to include these potential vulnerabilities into their reports

I was blind, but now I see!

As a suggestion to decrease the level of blindness of external scans and decrease the workload, companies should consider scanning external targets from the inside as part of their mandatory quarterly internal scans. This secured scan source allows for authenticated scans with full access to the targets and is therefore more reliable. Use the internal scan reports to quickly spot false positives in the external scan reports.

A second, but less practical, option is to establish an encrypted tunnel between the external scan source and the scanned network allowing for the use of authenticated checks.

#18 What to do if compromised?

Experience and statistics show us that the unlikely happens, we don't know when, we don't know how—but we know it will occur. So management should be concerned about being prepared to face an incident, rather than being secure alone.

"I'm compliant so I don't care."

The above principle has never been so true within the context of PCI, where compliance doesn't really shelter organizations from compromises and therefore penalties.

Achievement of PCI compliance is a long, costly, and fastidious journey to the promised land of immunity towards penalties. To avoid or minimize penalties, compromised companies must prove that they did everything they could to prevent, detect, report, and follow up on an incident in accordance with the "rules."

Payment Brands have stringent rules and fines related to incident reporting.

For instance, Visa is requiring their members (banks) to immediately report suspected or confirmed losses or theft of any transaction data. Members failing to do so are subjected to a $100,000 fine per incident + $50,000 for any merchant or service provider that is not compliant at the time of the incident.

As a merchant or service provider, what do I have to do?

Upon occurrence of a security breach and/or suspicion of compromised card data, an overwhelming sense of panic could paralyze any individual responsible for security and/or compliance. The fear of responsibilities and business impacts in terms of penalties and reputation could disconcert more than one person. As mentioned above, the compliance status at the time of the incident would not be sufficient to keep you sheltered against these fears. You have to act rapidly accordingly to the procedures. In this domain, as indicated by PCI DSS 12.9, preparation is key.

Req 12.9 of the PCI bible (PCI DSS) requires merchants and service providers to be prepared to respond immediately to a breach.

What are the procedures?

It's important to note that the payment brand reporting procedures and associated fines are applied to members (Banks) not the merchants and service providers. Unfortunately, there are no publicly available rules applicable for merchants and service providers in case of compromises. So my first advice would be to liaise with your bank to determine what these procedures are, establish associated milestones as well as specific reporting templates. Different procedures and report templates could be required for different payment brands. Act right now and don't wait for a compromise. You will not have the time.

Such procedures could include the following parts:

Contain, limit exposure, and monitor

- Do not access or alter compromised system(s). Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network
- Preserve evidence and logs
- Document all actions taken
- Be on high alert and monitor traffic on all systems with cardholder data

Alert all necessary parties immediately

- Internal incident response team
- Your bank (PCI contact)
- Law enforcement agency

Make inventory of compromised data

Make an inventory of potential compromised data and report it to your bank

Perform initial investigation and deliver breach report

Perform an initial investigation and provide a breach report to your bank. This report must help them understand the breach vectors and potential extent of the compromise as well as the actions taken to contain and limit exposure. For this investigation merchants could use their own internal resources or the services of a consulting company.

Is it mandatory to use a PFI (PCI Forensic Investigator)?

When deemed necessary by the payment brands, an independent forensic investigation could be required. In this case, the compromised organization must engage a PFI company and support the cost. The role of such a company is to investigate the case and verify the level of responsibility of the compromised entity.

References

VISA rules and procedures: What to do if compromised - For Acquirers and Issuers

#19 Your PCI Logbook - What is required in terms of log management?

P>D+R is a well-known principle in security.

It's a principle that means that the Protective measures in place must be strong enough to resist longer than the time required to Detect that something wrong is happening and then React.

For example, your door must be strong enough to prevent a malicious individual from getting in for at least the amount time required to detect the incident, alert the police, and have them arrive on site.

In this context, log management plays a specific role. It helps limit the risk of occurrence of incidents by detecting upstream suspicious activities. They help with understanding the *modus operandi* of incidents by tracking back the activities.

A little story. Four guards are instructed to watch the perimeter fence of your organization. The first one immediately falls asleep lulled by the silence of the night, the second one, a passionate writer, logs in his notebook every observation—including the presence of stars, clouds, the temperature and his state of mind. The third one, a bit stressed, rings the alarm bell every time he detects or hears "something."

Alert!

This is...oh...a rabbit. I'm sorry guys!

The fourth and last guard, an instructed and skilled professional, writes down specific events he learned to classify and awakes the garrison only in case of emergency.

As illustrated through the above scenario, audit trails have their own problems. They are useless if too quiet or too talkative and if they lack adequate monitoring. In other words, monitoring is inefficient if too scarce, too permissive or too alarming. To be efficient, audit trails must be configured appropriately and constantly reviewed.

In this domain, PCI DSS specifies what events must be logged (10.2) as well as what data must be recorded for each event (10.3). PCI DSS also addresses the protection of the audit trails (10.5) and audit files retention (10.7).

In terms of review, PCI DSS requires audit trails to be reviewed on a daily basis (10.6)—this is more prescriptive than the SANS Top 20 Critical Security Controls, which suggests "biweekly reviews." However, SANS goes further than PCI by suggesting the automation of this tedious process through the use of SIEM technology.

What is SIEM technology?

SIEM stands for "Security Information and Event Management."

It's the combination of SIM (Security Information Management) collecting information and doing some basic analysis and SEM (Security Event management) evaluating the collected information in search of defined security events.

What does SIEM technology do?

SIEM technology allows event logs to be automatically collected, centralized and managed (analyzed, filtered, classified and reported) such that security events are reported according to their level of risk. So, an SIEM could be perceived as a kind of "intelligent" robot that would observe what is going on, detect signs of aggression, generate reports, and ring the alarm bells in case of emergencies (upon detection of critical anomalies).

Technically PCI doesn't require or prevent the use of such technology, which carries its own problems as well. Some organizations achieve compliance in regards to log management without an SIEM, while for others, an SIEM technology is deemed necessary due to the high volume of logs.

How does a QSA validate compliance?

To validate implementation, Qualified Security Assessors (QSA) are required to perform interviews, review the related policies and procedures and samples log files. Organizations subjected to compliance must confirm implementation of the requirements during the interviews and show the policies and procedures related to log management as well as samples of audit logs.

About the Author: Didier Godart

Risk & Compliance Product Manager, Rapid7

Didier is a key actor of the PCI council from its early days. He set the first security rules for e-commerce security and co-authored the first versions of the PCI Data Security Standard and related self-assessment questionnaires. Didier also advised the PCI council on areas for enhancement and wrote the standard for Approved Scanning Vendors.

Notably, Didier also designed and led the ASV Certification Lab—a unique program aiming to leverage the expertise of scanning vendors through a consistent certification process in order to deliver a standardized and efficient added value to the e-community.

Didier is widely recognized in the security community for his contribution to the enhancement of the quality of scanning services and more specifically the security of e-commerce.

Didier is the author of the book: “Sécurité Informatique: Risques, Stratégies et Solutions,” a security awareness educational program which has been followed by more than 8,000 people to date. A frequent moderator and speaker at various seminars and conferences, Didier’s other works include a number of publications on information security and risk management, including the PCI Compliance Dashboard and the PCI 30-Seconds newsletters on SecurityStreet, the Rapid7 online community.